Utvikling og bruk av kritiske programmerbare systemer : en kartlegging av kompetanse og behov i norsk industri

Gustav Dahll
og Rune Winther

Høgskolen i Østfold
Rapport 2003:1

Online-versjon (pdf)

Utgivelsessted: Halden

Høgskolen i Østfold har en godkjenningsordning for publikasjoner som skal gis ut i Høgskolens Rapport- og Arbeidsrapportserier.

Rapporten kan bestilles ved
henvendelse til Høgskolen i Østfold.
(e-post: post-fa@hiof.no)

Kartleggingen er utført som et samarbeid mellom:
Kongsberg Simrad
Det Norske Veritas
Institutt for energiteknikk
Statens Jernbanetilsyn
Høgskolen i Østfold, Avd. for informatikk og automatisering
SINTEF

Rapporten er skrevet av:
Gustav Dahll, Institutt for energiteknikk
Rune Winther, Høgskolen i Østfold, Avd. for informatikk og automatisering

Prosjektet er støttet økonomisk av Norges Forskningsråd

Høgskolen i Østfold. Rapport 2003:1

ISBN: 82-7825-112-6
ISSN: 1503-2612

Forord

Kartleggingen som er dokumentert i denne rapporten er ment å være starten på en mer omfattende aktivitet i Norge når det gjelder kompetanseheving omkring utvikling og bruk av kritiske programmerbare systemer. Det er et faktum at vi både på samfunnsnivå og individnivå har blitt svært avhengige av programmerbare systemer. En del av disse systemene er også kritiske i den forstand at de ved å feile kan medføre stor skade, både helsemessig, miljømessig og økonomisk. Det er slike system som har vært fokusert i denne kartleggingen.

I Norge finnes det i dag ingen utdanningstilbud som har primærfokus på sikkerhet i systemer hvor programvare er en sentral del. Den forskningsaktiviteten som foregår er bra, men er i omfang alt for liten til å dekke alle sentrale problemstillinger. Når vi samtidig ser en sterk utvikling i retning av å ta i bruk programmerbare enheter vil norsk industri fort kunne komme på etterskudd i forhold til utenlandske konkurrenter når det gjelder å tilby systemer som kan brukes i potensielt kritiske anvendelser.

I 2000 tok Høgskolen i Østfold og Institutt for Energiteknikk (Halden) initiativ til å starte et landsdekkende nettverk, NONSTOPP, innenfor temaområdet ”sikre, trygge og pålitelige programmerbare systemer”. Det var med utspring i dette nettverket at dette kartleggingsarbeidet ble startet. Behovet for kartleggingen er begrunnet med at vi ikke har noen systematisk oversikt over norsk industris kompetanse når det gjelder dette temaområdet. Selv om vi fra egen erfaring har en formening om hvilke temaer det er nødvendig å forske mer på, ønsket vi med denne kartleggingen både å kartlegge utvalgte bedrifters kompetanse og de problemstillinger bedriftene selv mener er nødvendig å fokusere på i fremtiden. Det må understrekes at dette er en overordnet kartlegging, og ikke en detaljert eller komplett oversikt over norske bedrifter som utvikler eller bruker kritiske programmerbare systemer. Til tross for at en slik overordnet kartlegging åpenbart kan forbedres er vi av den oppfatning at videre ressurser heller burde brukes på konkrete forskningsprosjekter. Kartleggingen dokumentert i denne rapporten gir grunnlag for å definere konkrete forskningsprosjekter innen dette fagområdet. Ved å la slike forskningsprosjekter foregå i samarbeid mellom industribedrifter, forskingsinstitusjoner og universitet/høgskoler vil en oppnå ytterligere kunnskaper om hvilke behov som finnes og hvordan disse skal tilfredsstilles.

Innholdet av denne rapporten beskriver forfatternes vurderinger av de innkomne svar, og representerer derfor ikke noe offisielt synspunkt til prosjektdeltakernes institusjoner.

Sammendrag

Prosjektet:

Denne rapporten beskriver resultatet fra en kartlegging blant norske bedrifter når det gjelder utvikling og bruk av kritiske programmerbare systemer, dvs. systemer der sentrale funksjoner styres av programvare og som ved å feile kan medføre stor skade, både helsemessig, miljømessig og økonomisk.

Hovedmålet for prosjektet har vært å legge et grunnlag for styrking av kompetansen hos norske bedrifter når det gjelder utvikling og evaluering av programmerbare systemer som kan være av betydning for sikkerheten for mennesker og miljø. Et viktig element for å få til dette er å også styrke den generelle sikkerhetskompetansen på IKT-området i Norge gjennom forskning og utdanning. Dette vil øke konkurransekraften til deltakerne, såvel som norsk industri generelt, ved deltakelse på det internasjonale marked i prosjekter der IKT-sikkerhet er av betydning. Målsetningen med forprosjektet spesielt er å videreutvikle NONSTOPP-nettverket, kartlegge behov og kompetanse hos norske bedrifter, samt å skape et grunnlag for videre samarbeid mellom norske bedrifter gjennom et hovedprosjekt.

Resultatene er tenkt brukt til å identifisere aktuelle forskningstemaer, kompetansebehov og behov for utdanningstilbud. Selve prosjektet har også hatt den effekten at nye kontakter er knyttet, noe som kan utnyttes i seinere prosjekter.

Rapporten består av tre hoveddeler. Den første beskriver hvordan kartleggingsprosjektet er gjennomført. Den andre gir en beskrivelse og vurdering av de innkomne svar, mens den tredje inneholder observasjoner og konklusjoner.

I tillegg er det to appendikser som henholdsvis inneholder spørreskjemaet som ble sendt ut og de faktiske svarene.

Prinsippet for valg av bedrifter for intervjuer har vært å dekke et vidt spektrum av roller og markeder.

Et intervjuskjema som skulle brukes, samt en liste over bedrifter man ønsket skulle bli kartlagt, ble utarbeidet. Spørreskjemaet ble så sendt til de utvalgte bedriftene. Disse ble besvart, enten direkte skriftlig eller ved et intervju med en av prosjektdeltakerne. De innkomne svarene ble lagret og systematisert. For hvert spørsmål ble det laget tabeller med svarene fra hver bedrift.

Svarene på spørsmålene er gitt i tabeller i kapittel 3. For hver tabell (eller gruppe av tabeller der det er naturlig) er det gitt en kort tekst som beskriver de observasjonene en kan gjøre på grunnlag av besvarelsene. Disse observasjonene er gjengitt i kapittel 4, som også inneholder generelle

konklusjoner. Kapittel 5 inneholder noen forslag til forskningstemaer for videre FoU-innsats, basert på resultatene fra kartleggingen.

Resultater:

De viktigste observasjonene som er gjort på basis av svarene, kan oppsummeres som følger:

Noen bedrifter dekker flere markeder, mens noen konsentrerer seg om ett enkelt markedssegment. Imidlertid er alle de foreslåtte markedene, med unntak av medisinsk utstyr, dekket av minst én bedrift. Generelt dekker de bedriftene som har besvart spørreskjemaet et vidt spektrum, både når det gjelder rollekategori, marked og størrelse.

De fleste nevner tap av menneskeliv som (verst) mulig konsekvens ved feil i deres systemer. Det varierer mellom katastrofale følger (stort antall dødsfall) til enkeltpersoners skader, eventuelt død. Når det gjelder spørsmålet om det virkelig har skjedd ulykkeshendelser relatert til feilfunksjon av systemer kan svaret sammenfattes til: Ingen alvorlige, men muligens noen mindre hendelser. Miljøskader blir også nevnt, uten at de blir presentert nærmere. Alle nevner mulige økonomiske konsekvenser, noe som er naturlig for et system i aktivt bruk. Størrelsen varierer imidlertid stort, fra ca. 200 MNOK til manglende tilgjengelighet av systemet, og tap av tillit blant kunder.

De fleste utviklere av programmerbare system bruker standarder som grunnlag for programvareutvikling. Imidlertid brukes forskjellige standarder, både internasjonale standarder og bedriftsspesifikke standarder. Når det gjelder utviklingsmetodikk er svarene mer negative. Bare tre bedrifter nevner spesielle metoder.

Alle bedriftene foretar noen form for verifikasjon og validering av sine produkter. Svarene gir imidlertid ikke mange detaljer på hvordan det gjøres, og ingen nevner verktøy som brukes.

Kritiske programmerbare systemer har en bred anvendelse. Dette indikerer at det er behov for generelle prinsipper på dette området, som er anvendbare på mange typer systemer. Brukere av innkjøpt programvare setter generelt krav til kvalitetssikring hos produsenter/leverandører. Det virker som forskjellige bedrifter bruker forskjellige standarder, men det er mulig at de underliggende prinsippene ikke er så forskjellige.

Svarene indikerer også at alle brukerbedriftene har gode rutiner for drift og vedlikehold. Dette inkluderer også rapportering av problemer.

Det stilles generelle sikkerhetskrav til kritiske systemer, men i mindre grad stilles spesielle sikkerhetskrav til programvare. Dette reflekterer det syn at det

er systemer som sådan, og ikke programvaren som vil være en potensiell sikkerhetsrisiko.

Bedriftene utarbeider sikkerhets- og pålitelighetskrav til kritiske system, basert på risikoanalyser og behov for risikostyring og risikoreduserende tiltak. Dette gjøres ofte i samarbeid med en kunde. De fleste svarer også positivt på om det utarbeides en samsvarsvurdering i henhold til gitte sikkerhetskrav.

De fleste bedriftene gjennomfører pålitelighets/risiko-analyser av kritiske systemer, og mener at deres systemer kan anvendes i kritiske applikasjoner.

Etter en ulykke vil det i de fleste tilfelle foretas en granskning av hva som var årsaken til ulykken, og hva som vil kunne gjøres for å hindre liknende ulykker i framtida. For de fleste vil det være mulig å spore tilbake hvordan det programmerbare systemet fungerte før og under hendelsen.

Det kommer klart fram fra svarene at alle bedrifter ønsker å øke sin kompetanse for alle faser i utviklingen av kritiske programmerbare systemer. Kravspesifikasjonen er klart det området der behovet for styrking av kompetanse er størst, mens produksjon, utvikling og operasjon kommer i den andre enden. Dette avspeiler kanskje at det er disse siste områdene bedriftene har satset mest på, eller at kravspesifikasjonen er den viktigste og vanskeligste fasen, den som krever mest kompetanse for å utføres tilfredsstillende.

Svarene viser videre at spesialutdanning av sikkerhetsansvarlige og kursvirksomhet er de mest anbefalte metodene innenfor kompetansestyrking innen bedriften, mens utdanningstilbud er viktigst i Norge generelt.

Når det gjelder framtidig forskning hadde ikke alle bedriftene klare meninger om hvilke problemstillinger de synes er viktigst. Imidlertid uttrykker alle at de er interessert i å være med i et forskningsprosjekt, enten i en indre kjerne eller i en ytre referansegruppe. De fleste er i prinsippet interessert i å delta i en indre kjerne.

Innhold

Tabeller

1 Innledning

Dette kapittelet beskriver bakgrunn og formål med prosjektet, samt gir en oversikt over deltagerne i prosjektet.

1.1 Bakgrunn for prosjektet

I den seinere tid har sikkerhetsproblematikk kommet i fokus innen en rekke viktige samfunnsaktiviteter, noe som bl.a. har ført til oppnevnelsen av det såkalte Sårbarhetsutvalget og deres rapport NOU 2000:24 ”Et sårbart samfunn”. Den økende bruk, og avhengighet av IKT- systemer medfører at sikker bruk av slike systemer er et vesentlig aspekt i denne sammenheng. Derfor ble et nasjonalt nettverk NONSTOPP (NOrsk Nettverk for Sikre, Trygge og Pålitelige Programmerbare systemer) startet i 2000, og et seminar om "Sikker bruk av programmerbare systemer" ble arrangert i Halden i september samme år. Basert på inntrykkene fra seminaret og egne erfaringer etablerte en gruppe av deltakerne i NONSTOPP en prosjektgruppe som skulle planlegge videre innsats på dette området. Denne gruppen søkte og fikk finansiell støtte fra NFR til et forprosjekt som ble gjennomført i 2001.

1.2 Målsetningen for prosjektet

Hovedmålet for prosjektet har vært å legge et grunnlag for styrking av kompetansen hos norske bedrifter når det gjelder utvikling og evaluering av programmerbare systemer som kan være av betydning for sikkerheten for mennesker og miljø. Et viktig element for å få til dette er å også styrke den generelle sikkerhetskompetansen på IKT-området i Norge gjennom forskning og utdanning. Dette vil øke konkurransekraften til deltakerne, såvel som norsk industri generelt, ved deltakelse på det internasjonale marked i prosjekter der IKT-sikkerhet er av betydning. Målsetningen med forprosjektet spesielt er å videreutvikle NONSTOPP nettverket, kartlegge behov og kompetanse hos norske bedrifter, samt å skape et grunnlag for videre samarbeid mellom norske bedrifter gjennom et hovedprosjekt.

Hovedaktiviteten i forprosjektet har vært kartlegging av status og behov hos norske bedrifter som leverer eller bruker kritiske programmerbare systemer. Resultatene er tenkt brukt til å identifisere aktuelle forskningstemaer, kompetansebehov og behov for utdanningstilbud. Selve prosjektet har også hatt den effekten at nye kontakter er knyttet, noe som kan utnyttes i senere prosjekter.

1.3 Strukturen på rapporten

Rapporten består av tre hoveddeler. Den første beskriver hvordan kartleggingsprosjektet er gjennomført. Den andre gir en beskrivelse og

vurdering av de innkomne svar, mens den tredje inneholder observasjoner og konklusjoner. I tillegg inneholder rapporten noen forslag til forskningstemaer for videre FoU-innsats, basert på resultatene fra kartleggingen.

I tillegg er det to appendikser. Appendiks A inneholder spørreskjemaet som ble sendt ut. Appendiks B inneholder de faktiske svarene. Av hensyn til konfidensialitet er imidlertid ikke bedriftene koplet til svarene, og rekkefølgen av svarene innen de forskjellige tabellene er randomisert for å hindre sporbarhet.

Det må imidlertid understrekes at dette er en *kartlegging* og ikke er en vitenskapelig undersøkelse der hypoteser bekreftes eller avkreftes. Den begrensede størrelsen på dette prosjektet gjør at noen statistisk bearbeiding av materialet ikke vil være korrekt å utføre. Observasjoner og konklusjoner er gjort på en ad hoc basis av forfatterne av denne rapporten. Det er derfor lagt vekt på å ta med alt materialet fra svarerne i appendiks B, slik at andre lesere kan gjøre egne observasjoner og konklusjoner. Vi vil, imidlertid, som nevnt over, i forbindelse med konklusjonen formulere noen forslag til videresatsing basert på denne kartleggingen.

1.4 Prosjektdeltagere

Deltagerne i dette prosjektet består av organisasjoner og personer som deltok aktivt i det første NONSTOPP-seminaret som ble arrangert i september 2000. Deltagergruppen inkluderer både produsent-, konsulent-, tilsyns- og forskningsmiljøer og dekker således en rekke forskjellige perspektiver når det gjelder temaet sikre og trygge programmerbare systemer. De deltagende organisasjoner, inklusive kontaktpersoner og deres hovedansvarsområder i dette prosjektet, er gitt i følgende tabell.

Organisasjon	**Kontaktpersoner**	**Ansvarsområder**
Det Norske Veritas	Stian Ruud	• Planlegging av kartleggingsarbeidet • Intervju av utvalgte bedrifter • NONSTOPP-seminar
Høgskolen i Østfold	Rune Winther	• Planlegging av kartleggingsarbeidet • Intervju av utvalgte bedrifter • Skriving av rapport • NONSTOPP-seminar
Institutt for energiteknikk	Gustav Dahll Thorbjørn Bjørlo	• Planlegging av kartleggingsarbeidet • Intervju av utvalgte bedrifter • Skriving av rapport

		• Prosjektledelse
Statens Jernbanetilsyn	Knut Rygh	• Planlegging av kartleggingsarbeidet
Kongsberg Simrad	Øyvind Lyftingsmo	• Planlegging av kartleggingsarbeidet • Prosjektansvarlig
SINTEF	Øystein Skogstad	• Planlegging av kartleggingsarbeidet • Intervju av utvalgte bedrifter

BEGREPSDEFINISJONER

Begrep	Forklaring
Designer	En som utformer et programmerbart system, men ikke nødvendigvis deltar i implementasjon eller testing.
DO-178B	RTCA/DO-178B: “Software Considerations in Airborne Systems and Equipment Certifications”, (1992).
Entreprenør/integrator	En som setter sammen og leverer programmerbare systemer basert på innkjøpte komponenter.
FAT	Factory Acceptance Test
FMEA/FMECA	Failure Mode and Effect (and Criticality) Analysis.
Hyllevare	Programmerbare systemer som kan kjøpes kommersielt og brukes direkte av kjøperen (Commercial Off The Shelf (COTS)).
IEC-61508	"Functional safety of electrical/electronic/ programmable electronic safety-related systems". IEC Standard 61508.
IKT	Informasjons- og kommunikasjonsteknologi.
ISO-9000	En serie av kvalitetsstandarder.
Kritisk system	Et system der en feil kan få alvorlige konsekvenser for liv, helse miljø og/eller økonomi.
MIL-882D	MIL standard 882D: Mishap Risk Management (System Safety) US DoD Standard Practice.
NONSTOPP	NOrsk Nettverk for Sikre, Trygge Og Pålitelige Programmerbare systemer.
OPC	OPC (OLE for Process Control) er en teknisk spesifikasjon som definerer et sett av standard grensesnitt basert på Microsoft’s OLE/COM teknologi.
Produsent	En som har ansvaret for utvikling og produksjon av et programmerbart system.
Programmerbart system	System hvor programvare styrer en sentral del av systemets funksjonalitet.
ROSE	Et utviklingsverktøy for programmerbare systemer.
RUP	Rational Unified Process (en itereativ utviklingsprosess).
Samsvarsvurdering	En vurdering om et system er utviklet i samsvar med gitte krav.
SAT	Site Acceptance Test
Sikkerhet	Sikkerhet er i denne rapporten brukt synonymt med det engelske ”safety”, viz. fravær av fare for mennesker, for miljø eller for store økonomiske tap.

Sikkerhetskritisk	Er i denne rapporten brukt synonymt med kritisk.
SIL	Safety Integrity Level (definert i IEC-61508). Spesifiserer maksimalt akseptabel sannsynlighet for svikt i sikkerhetsfunksjon.
Testing	Eksekvering av et program med et sett av inngangsdata for å vise at det utfører den ønskete funksjonen rett, og at det ikke oppstår uønskete side-effekter.
Validering	Bekreftelse av overensstemmelse mellom et systems virkemåte og kravene til systemet under gitte betingelser.
Vedlikeholder	En som primært arbeider med å oppdatere/korriger eksisterende programvare.
Verifikasjon	Påvisning av at en fase i utviklingen av et system er i overensstemmelse med kravene stilt i foregående fase.
V-modell	En utviklings og verifikasjons modell basert på e sekvensielt utviklingsløp.
UML	Unified Modelling Language (en notasjon for software design).

2 Gjennomføring av kartlegging

I dette kapittelet beskrives prinsipper for valg av bedrifter, prosedyre for gjennomføring av intervjuer og hvordan vi har gått frem i oppsummeringen av de innsamlede data.

2.1 Utarbeiding av spørreskjema

Spørsmålene i spørreskjemaet ble valgt ut fra den hensikt å innhente mest mulig informasjon fra bedriftene angående utvikling og bruk av kritiske programmerbare systemer. Spørsmålene var ment å dekke forskjellige aspekter:

- *Bedriftsprofilene* for å få klarhet i om svarene dekket bedrifter innen flest mulig relevante markeder, roller og størrelser.
- *Praksis,* dvs. hvilken praksis de forskjellige bedriftene i dag følger ved utvikling og bruk av kritiske programmerbare systemer.
- *Sikkerhet,* dvs. hva bedriftene gjør for at systemene de utvikler eller bruker skal være sikre i bruk.
- *Behov,* dvs hvilke behov eller ønsker bedriftene har til kompetanseheving, og hvordan dette skal kunne oppnås gjennom undervisning og forskning.

Som nevnt tidligere, er *ikke* spørsmålene laget med hensikt på statistisk analyse. Formålet har heller vært å formulere et grunnlag for framtidige forskningsprosjekter gjennom å identifisere de temaene som har størst betydning.

I ettertid er det lett å se at enkelte spørsmål ikke har vært optimale, noe som i enkelte tilfelle har gjort det vanskelig å tolke svarene. Dette aspektet er kommentert videre i kapittel 4.1.

2.2 Valg av bedrifter for kartlegging

Prinsippet for valg av bedrifter for intervjuer har vært å dekke et vidt spektrum av roller og markeder. De rollene som ble identifisert som spesielt interessante var:

1. Designer
2. Produsent
3. Bruker/operatør
4. Entreprenør/integrator (en som setter sammen og leverer programmerbare systemer basert på innkjøpte komponenter)
5. Vedlikeholder

I tillegg til å dekke forskjellige roller ønsket prosjektet også å dekke et vidt spekter av markeder:

1. Olje/gass
2. Energiproduksjon/energiforsyning
3. Transport (luftfart, skipsfart, tog, veitransport)
4. Prosessindustri
5. Telecom
6. Data/informasjonsbehandling
7. Forsvar
8. Medisinske produkter
9. Produsent av utviklings/analyseverktøy (software og/eller hardware)

Det bør bemerkes at det ikke er gjort noe forsøk på å kartlegge alle norske bedrifter som leverer eller bruker kritiske programmerbare systemer. På grunn av prosjektets begrensede omfang, samt det faktum at kravene til sikkerhet vil være like for alle bedrifter i samme marked, ble kun et utvalg av bedrifter fra forskjellige markeder inkludert i kartleggingen. Dette anses å være tilstrekkelig for å få et godt bilde av den generelle situasjonen og de behov som finnes.

Selve utvelgelsen av aktuelle bedrifter ble gjort i fellesskap i prosjektgruppen basert på deltagernes kunnskaper og kjennskap til aktuelle bedrifter. All den tid deltagerne selv representerer forskjellige markeder og roller ble dette ansett som godt nok.

2.3 Prosedyre for gjennomføring av intervjuer

Prosjektgruppen utarbeidet i fellesskap et intervjuskjema som skulle brukes i kartleggingen (vedlagt i appendiks A), samt en liste over bedrifter man ønsket skulle bli kartlagt.

Spørreundersøkelsen ble utført etter følgende prosedyre:

- En forespørsel ble sendt til de utvalgte bedrifter om de kunne tenke seg å være med på undersøkelsen. Det ble også bedt om å få oppgitt en kontaktperson.
- Etter en tid ble disse bedriftene kontaktet, og de som svarte positivt fikk tilsendt spørreskjemaet. Det ble gjort oppmerksom på at svarene ville bli behandlet konfidensielt.
- Noen av spørreskjemaene ble besvart skriftlig. Andre ble besvart ved et intervju med en av prosjektdeltakerne, enten via telefon eller ved personlig oppmøte.
- De innkomne svarene ble lagret og systematisert. For hvert spørsmål ble det laget tabeller med svarene fra hver bedrift.

2.4 Prosedyre for rapportering av kartleggingen

Med et såvidt lite antall intervjuede bedrifter har vi for alle spørsmål valgt å inkludere svarene fra hver enkelt bedrift. Dette er for å gi leseren full tilgang til den informasjonen som danner grunnlag for våre konklusjoner. For de spørsmålene hvor det finnes et begrenset antall svaralternativer har vi i tillegg til enkeltsvarene foretatt en oppsummering av antall svar for hver alternativ. Alle konklusjoner er basert på kvalitative vurderinger av svarene samt prosjektgruppens egne erfaringer og kunnskap om de aktuelle temaene.

Svarene på spørsmålene er gitt i tabeller appendiks B. Et sammendrag av svarene er gitt i kapittel 3 der det også er korte tekster som beskriver de observasjonene en kan gjøre på grunnlag av besvarelsene. Disse observasjonene er gjengitt i kapittel 4, som også inneholder generelle konklusjoner.

3 Resultater fra kartleggingen

I dette kapittelet presenteres resultatene fra selve kartleggingen, oppsummert innenfor et sett hovedtemaer.

3.1 Respons fra bedriftene

De fleste bedriftene som fikk forespørsel ga en respons, enten ved å besvare spørsmålene, eller ved å gi et generelt svar at spørsmålene var irrelevante for deres bedrift. I noen få tilfeller fikk vi ikke gjennomført intervjuer som planlagt på grunn av manglende respons fra bedriftene. Totalt ble spørreskjemaet besvart av følgende 14 bedrifter:

- ABB-AS/Robotics
- Hydralift ASA
- Jernbaneverket
- Kongsberg Defence and Aerospace
- Maritime Hydraulics
- Bane Partner
- Park Air Systems
- Prediktor
- Kongsberg-Seatex
- Konsberg Simrad
- Statoil UPN TO DVT AUT
- SAAS System AS
- Telenor Network Services
- Viken Energinett AS

3.2 Beskrivelse av de utvalgte bedriftene

Dette kapitlet gir en generell beskrivelse av de bedriftene som har blitt intervjuet og de systemer de utvikler/bruker. Det bør bemerkes at hensikten ikke er å trekke konklusjoner for hvert enkelt marked eller rolle, men for å vise i hvilken grad målsetningen om å dekke et vidt spektrum er nådd.

3.2.1 Roller, markeder og størrelse

Tabell 1 gir en oversikt over hvor mange bedrifter som finnes i hver rollekategori, mens Tabell 2 gir en tilsvarende oversikt for markeder. En mer detaljert beskrivelse av hvordan de enkelte bedriftene dekker de forskjellige kategorier av roller og markeder er gitt i Tabell 21 i appendiks B. Som en ser er det noen bedrifter som dekker mange flere markeder, mens andre er mer konsentrerte på ett marked. Tabell 1 viser at de fleste rollene, med unntak av konsulenter, er rimelig godt dekket.

Rolle	Antall bedrifter
Designer	11
Produsent	10
Bruker/operatør	5
Entreprenør/integrator	7
Vedlikeholder	9
Konsulent, 3. parts verifikasjon, sertifisering	3

Tabell 1: Antall bedrifter som dekker de forskjellige kategoriene

Tabell 2 (og Tabell 21 i appendiks B) viser at noen bedrifter dekker flere markeder, mens andre konsentrerer seg om ett enkelt markedssegment. Tabell 2 viser at alle de foreslåtte markedene, med unntak av medisinsk utstyr, er dekket av minst én bedrift.

Det tredje aspektet av generell natur gjelder størrelsen på bedriftene. Dette er oppsummert i Tabell 3, mens detaljene i svarene er gitt i Tabell 22 i appendiks B. Da imidlertid noen av bedriftene er meget store, har det også vært av interesse å vite hvor mange som er relatert til utvikling eller bruk av kritiske programmerbare systemer. Dette er vist i en egen kolonne i tabellen.
Det er imidlertid uklart om alle bedriftene har tolket dette likt, både når det gjelder sikkerhetskritisk og når det gjelder programmerbare systemer. Resultatet må derfor tolkes med forsiktighet. Det er f.eks. neppe realistisk at en enkelt bedrift har 800 personer som har arbeid som er direkte relatert til utvikling eller bruk av kritisk programvare. Man må huske at et programmerbart system nødvendigvis også må bestå av ”hardware” av mange slag og at det derfor kan være vanskelig å definere et klart skille. Skillet mellom deltagelse i utvikling eller bruk av slike systemer er heller ikke spesifisert.

Marked	Antall bedrifter
Olje/gass	6
Energiproduksjon/energiforsyning	2
Transport	9
Prosessindustri	3
Telecom	2
Data/informasjonsbehandling	1
Forsvar	2
Produsent av utviklings/ analyseverktøy	1
Medisin	1
Annet	2

Tabell 2: Antall bedrifter som dekker de forskjellige markedene

Bedriftens størrelse i Norge	Antall bedrifter
1-50	2
51-200	2
201-1000	7
>1000	3

Antall ansatte som utvikler eller bruker kritiske programmerbare systemer	Antall bedrifter
1-10	2
11-50	6
51-100	1
>100	4

Tabell 3: Antall ansatte totalt og antall ansatte som utvikler eller bruker kritiske programmerbare systemer

En konklusjon på dette kapitlet er at de bedriftene som har besvart spørreskjemaet dekker et vidt spektrum, både når det gjelder rollekategori, marked og størrelse. Dette betyr at denne kartleggingen bør kunne gi et rimelig godt bilde av nå-situasjonen for norske bedrifter som utvikler eller bruke kritiske systemer.

3.2.2 Typer av systemer

Dette kapitlet vil vektlegge de sikkerhetskritiske aspektene ved systemer hos bedriftene, både de generelle og de som gjelder programmerbare systemer.

Tabell 23 i appendiks B viser hvilke type funksjoner som utøves av de kritiske systemene, sortert etter antall bedrifter som nevner systemet. Som en ser, så er spesielt kontroll/prosesstyring, men også nedstenging, kommunikasjons, brann- og gassdeteksjon og signalsystem nevnt av flere bedrifter, mens resten er spesielle systemer. Slik har en fått fram både konsentrasjon og spredning i svarene når det gjelder system. Fordelingen bærer også preg av at prosessindustrien er en viktig bruker av programmerbare systemer.

Type system	Antall bedrifter som nevner systemet
Kontroll/prosesstyring	8
Nedstengning	4
Deteksjon	3
Kommunikasjonssystem	3
Brann og gass deteksjon	2
Signalsystem	2
Automatisk togstopp	1
Bakkeradar	1
Brannpumpekontroll	1
Bremsesystem	1
Fakkelsystem	1
Komponenter for posisjonering	1
Konfigurering av telenett	1
Luftfartsovervåking	1
Manøvrere/sperre aktuatorer	1
Maskinstyring	1
Operatørstøttesystem	1
Posisjonering	1
Robot systemer	1
Romfart	1
Satellittnavigasjon	1
Trykkavlastningssystemet	1
Våpenkontroll	1

Tabell 4:Typer av systemer som er nevnt av bedriftene

3.2.3 Konsekvenskategorier av feil

Tabell 5 gir en oppsummering av konsekvenskategorier for feil i systemene (se også kolonne 1 av Tabell 24 i appendiks B). Som en ser nevner 11 av de 14 tap av menneskeliv som (verst) mulig konsekvens. Det varierer mellom katastrofale følger (stort antall dødsfall) til enkeltpersoners skader, eventuelt død. Når det gjelder spørsmålet om det virkelig har skjedd ulykkeshendelser relatert til feilfunksjon av systemer kan svaret sammenfattes til: Ingen alvorlige, men muligens noen mindre hendelser.

Konsekvenser av feil i systemene	Antall bedrifter
Menneskeliv/helse	11
Miljøskade	8
Økonomiske verdier	14

Tabell 5: Oppsummering av konsekvenskategorier for feil i systemene

Åtte nevner miljøskader, uten at de blir presentert nærmere. Alle nevner mulige økonomiske konsekvenser, noe som er naturlig for et system i aktivt bruk. Størrelsen varierer imidlertid stort, fra ca. 200 MNOK til manglende tilgjengelighet av systemet, og tap av tillit blant kunder.

3.3 Praksis ved utvikling og bruk av kritiske programmerbare systemer

Dette kapitlet fokuserer på hvilken praksis de forskjellige bedriftene følger ved utvikling og bruk av kritiske programmerbare systemer.

3.3.1 Utviklingsmetodikk

Dette avsnittet behandler aspekter relatert til utvikling av kritisk programvare. Bedriftene som har besvart spørreskjemaene omfatter både hyllevareprodusenter og systemprodusenter. Tabell 6 gir en oversikt over forskjellige svar gitt på spørsmål angående utviklingsstandard og utviklingsmetodikk.

Baserer dere utviklingen på noen spesifikk standard? Hvis ja, hvilken?	Brukes det noen spesiell utviklings-metodikk? Hvis ja, hvilken?
Referer til ISO 9000-3, ISO 9000-7	nei
Egen QA prosedyre	Egenutviklet prosess anvendes
DO 178B, IEC 61508, Eurocontrol/ANSSAM	V-modell
Bruker en metode basert på ”Unified software development process” (minner om RUP)	som første kolonne
EN 50128, EN 61508	-
IEC 61508	RUP, UML, ROSE
ISO & EN,ANSI sikkerhets standarder relatert til våre systemer	nei
Interne utviklingsstandarder	SLATE system engineering.
Nei, bare i spesielle tilfeller. Kundekrav	UML

Tabell 6: Bruk av standarder og utviklingsmetodikk

De fleste produsentene baserer utviklingen på en spesifikk standard. Det varierer mellom internasjonale standarder og bedriftsspesifikke standarder. Selv om bedriftene bruker forskjellige standarder for systemutvikling, er det mulig at de underliggende prinsippene ikke er så forskjellige.

På spørsmålet om det brukes en spesiell utviklingsmetodikk er imidlertid svarene, selv blant de som svarer positivt, av blandet karakter. En av grunnene til dette kan være at begrepet *utviklingsmetodikk* ikke er klart definert, og at det for noen kan være vanskelig å skille mellom dette og begrepet *standard.* Mens noen nevner spesifikke utviklingsprosesser (RUP) nevner andre spesifikk notasjon (UML) og konkrete verktøy (ROSE). Selv om det er rimelig å fortolke disse svarene dithen at de fleste har et bevisst forhold til hvordan utvikling skal foregå er det vanskelig å danne seg et klart bilde av hva slags prosesser og metoder de benytter seg av.

3.3.2 Pålitelighetsaspekter

Dette avsnittet tar for seg forskjellige aspekter når det gjelder pålitelighet og korrekthet av programvare. Svar på spørsmål om pålitelighetsmål og –data er gitt i Tabell 7. Dette er bare relevant for utviklere av kritisk programvare. Fem av bedriftene svarte klart ja, men spørsmålet kan være uklart, dvs. om pålitelighetsmålene også omfatter programvaren. Når det gjelder pålitelighetsdata for programvare vil dette innebære logging med detaljert beskrivelse av programfeil som er oppdaget, og eventuelt rettet.

Settes det mål for pålitelighet?	
Ja	5
Nei	5

Kan pålitelighetsdata produseres?	
Ja	5
Delvis	4
Nei	1

Tabell 7: Antall bedrifter som setter mål for pålitelighet og som kan produsere pålitelighetsdata

Tabell 8 og Tabell 9 gir en oversikt over forskjellige svar på spørsmål angående verifikasjon og validering, inkludert testing. Alle bedriftene foretar noen form for verifikasjon og validering av sine produkter, men svarene gir ikke mange detaljer på hvordan det gjøres, og ingen nevner verktøy som brukes. Om dette betyr at de ikke bruker hjelpeverktøy er uklart.

Når det gjelder testing synes det som bedriftene kan deles i to grupper, de som planlegger testen fra begynnelsen, basert på funksjonsspesifikasjoner, og de som lager testprosedyrene på et seint stadium, rett før testen skal utføres. En vanlig oppfatning er at testspesifikasjonen bør gjøres på et tidlig tidspunkt, samtidig med kravspesifikasjonen. Det er imidlertid ting som taler imot dette. Utviklerne kan bruke dette som ’fasit’, og konsentrere seg om å tilfredsstille denne istedenfor å konsentrere seg om kravspesifikasjonen og de behov systemet skal møte. Feil i akseptansetest er også en kjent feilkilde. Det ville

være interessant å vite om valgene av teststrategi var gjort bevisst, samt å sammenlikne erfaringer mellom disse framgangsmåtene i en framtidig studie.

Foretas noen verifikasjon og/eller validering av programmene? I tilfelle, hvordan? Hvilke verktøy
Ja for visse systemer, sjelden for andre
Følger kravstandarden OPC
Ja, dersom installasjonen skal godkjennes av en uavhengig assessor
Gransking og testing
Risikoanalyser, følger opp, sporbarhet
Stor variasjon, noe innebygget validering i PLS styringer, noe verifikasjon av FMECA
Intern verifikasjon, aldri møtt krav om 3. partsverifikasjon/samsvarsvurdering
Ja, lab-tester
Selvtester, sertifisert software, 3 part
Ja. MIL-882D krever dette. Det blir foretatt en pålitelighetsanalyse for å verifisere at systemer tilfredsstiller pålitelighetskrav

Tabell 8: Verifikasjon og validering

Når skrives testprosedyrene og gjennomføres testing etter en testplan?
Ved funksjonspesifikasjon
Før vi starter programmering
I designfase og gjennomføres på (FAT) og på commissioning
FAT og SAT-testing. Bruker standard maler for testing
Testprosedyrene skrives rett før test. Testplan finnes
na
Tidlig i utviklingsfasen
I praksis sent
Ved utarbeidelse av spesifikasjoner
Vanligvis for sent i prosessen

Tabell 9: Testprosedyrer

3.3.3 Bruk av systemer

Dette avsnittet behandler aspekter relatert til brukere av kritisk programvare. Bedriftene som har besvart spørreskjemaene omfatter både systemprodusenter som bruker andres programvare, og rene brukere.

Tabell 10 og Tabell 11 gir en oppsummering av svarene (se Tabell 26 i appendiks B) på spørsmålene angående hvilke krav som stilles til leverandør

av programvare og til innkjøpt programvare. Da svarene ikke alltid har samme ordlyd, er de tolket inn i de hovedkategoriene som er gitt i tabellene.

Hvilke krav stiller dere til leverandør av programvaren?	**Antall svar**
Kvalitetssikring/sertifisering	6
Utviklingsmetodikk/ følger standarder	5
Erfaring	3
Utviklingsmetodikk i forhold til sikkerhet	2
Tidligere leveranser av programmer i sikkerhetskritisk anvendelse	1
Lager de fleste komponenter selv. Kan bli bedre til å stille krav til underleverandører	1

Tabell 10: Oppsummering av krav til leverandør

Hvilke krav stiller dere til innkjøpt programvare?	**Antall svar**
Oppfylling av standarder/regelverk	6
Verifikasjon/testing	5
Dokumentasjon av relevante data (versjons-historie, logging av feildata, brukererfaring)	5
Forbedringspotensiale	2
Programdokumentasjon	1
Dokumentasjon av relevante data (versjons-historie, logging av feildata, brukererfaring)	1

Tabell 11: Oppsummering av krav til innkjøpt programvare

Brukere av innkjøpt programvare setter generelt krav til kvalitetssikring hos produsenter/ leverandører. Det virker imidlertid som forskjellige bedrifter bruker forskjellige standarder for disse kravene, men det er mulig at de underliggende prinsippene ikke er så forskjellige. Det som imidlertid er betegnende er at det ikke er noen standardisert måte å gjøre dette på som er felles på tvers av bedriftene.

Følgende fire spørsmål ble stilt til de som representerte brukere:

- Har brukerne kjennskap til forutsetninger for bruk av systemene?
- Har brukerne fått opplæring i nødvendig oppfølgning mht behov for å identifisere nødvendig vedlikehold?
- Logges og rapporteres faresituasjoner under drift?
- Logges driftsproblemer og erfaringer med systemer under drift?

Alle brukerne svarte ja på disse spørsmålene. Dette indikerer at brukerbedriftene alle har gode rutiner for drift og vedlikehold. Dette

inkluderer også rapportering av problemer. Det siste kan være av betydning hvis en ønsker å lage en problemdatabase for programvare. En interessant observasjon er at der er generelt en bedre håndtering av drift/vedlikehold enn av krav og testing. Dette kan ha sammenheng med at tidsnød eller krav til kostnadsbesparing ofte preger utvikling av nye system

3.4 Sikkerhetsaspekter

Sikkerhet ved bruk av programmerbare systemer har vært et vesentlig aspekt ved kartleggingen. Derfor var også mange av spørsmålene fokusert på dette. Dette gjelder både hvilke sikkerhetskrav som stilles, og hva bedriftene gjør for å oppfylle disse kravene.

3.4.1 Gjeldende sikkerhetskrav

Det ble stilt spørsmål om sikkerhetskrav, såvel generelle som til programmerbare systemer, fra myndigheter og fra bruker/kjøper/samarbeidspartnere. Når det gjelder generelle krav fra myndighetene er svaret bekreftende fra alle bedrifter unntatt én. Alle svarene er gitt i Tabell 27 i appendiks B. En sammenfatning av generelle krav som myndighetene krever skal være oppfylt innen forskjellig områder svarbedriftene omfatter er gitt i Tabell 12, mens en sammenfatning av spesielle myndighetskrav til programmerbare systemer er gitt i Tabell 13.

Når det gjelder om myndighetene stiller spesielle krav til sikkerheten i de programmerbare systemene, var svarene langt mer uklare. I stor grad gjelder de generelle kravene også for programmerbare systemer. Spesielle krav som er nevnt er at standardene DO-178B eller IEC-61508 skal følges, at det ikke skal være to barrierer på samme CPU, samt en del krav spesielt for kraftforsyningen. Imidlertid poengterer flere at de forventer mer spesifikke krav i framtida.

Militære standarder
Luftfartsverkets standarder for luftfartssystemer
Oljedirektoratets regelverk
Sjøfartsdirektoratets regelverk
Personvernmessige krav
Forskrift for elektriske anlegg - Forsyningsanlegg (FEA-F)
Forskrift om sikkerhet ved arbeid i og drift av høyspenningsanlegg med veiledning (FSH)
Forskrift om sikkerhet ved arbeid i og drift av lavspenningsanlegg (FSL)
Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid (IK)
Forskrift om elektrisk utstyr (FEU)
Forskrift om kvalifikasjoner for elektrofagfolk med veiledning (FKE)
EU direktiver
Jernbaneloven, inkl. forskrifter

Sokkelstatskrav
Den Nye Internasjonale Sikkerhetsstandarden IEC 61508, introdusert gjennom OD-veiledning 070 (– OLF Guideline for IEC61508 og IEC 61511)
ISO og EN standarder mht sikkerhet

Tabell 12: Generelle krav som myndighetene krever/anbefaler skal være oppfylt

MIL 882D
DO-178B luftfartssystemer
Redundans og sikkerhetsbarrierer. Ikke to barrierer på samme CPU
Sikkerhetsbestemmelser og beredskapshåndbok for kraftforsyningen
"Direktiv for sikring av datasystemer gradert etter Sikkerhetsinstruksen eller Beskyttelsesinstruksen", gitt av Forsvarssjefen 28 januar 1998
Enkeltfeil skal ikke føre til tap av menneskeliv eller alvorlig personskade
Jernbaneloven med tilhørende forskrifter, spesielt forskrift av 23.12.00
OD-veiledning 070 (– OLF Guideline for IEC61508 og IEC 61511). Flere krav vil fremtvinge seg
ISO og EN standarder mht sikkerhet

Tabell 13: Spesielle myndighetskrav/anbefalinger til programmerbare systemer

Samme spørsmål ble stilt angående brukers/kjøpers/samarbeidspartneres krav til sikkerhet. Alle svarene er gitt i Tabell 28 i appendiks B. En sammenfatning av svarene er gitt i Tabell 14 og Tabell 15. Når det gjelder spesielle krav til sikkerheten i de programmerbare systemene, var svarene her, som når det gjelder myndighetskrav, at det enten ikke er noen slike spesielle krav, eller at de generelle krav skal følges. FAT og SAT tester blir nevnt.

Militære setter krav til oppfylling av militære standarder
Enkelte kunder, som Lockhead Martin og Raytheon, bruker sine egne sikkerhetskrav
For romfart brukes ECSS-standarden
ISO og EN standarder mht sikkerhet
Oppfyllelse av SIL- nivåer definert i EN50129
Driftsstabilitet, krav til tilgjengelighet/oppetid
Noen operatører stiller flere og strengere krav enn myndigheter
Lov, forskrifter, Europanormer
Datasikkerhet (brannmur, inntrenging etc.) i tillegg til pålitelighet/oppetidskrav
Samme krav som myndighetene
generelle krav til funksjon og konstruksjon gjort med tanke på å unngå ulykker

Tabell 14: Bruker/kjøper/samarbeidspartneres krav til sikkerhet

Brukerne stiller stort sett generelle sikkerhetskrav, ikke spesifikt for programvare
FAT og SAT.
Krav til brukerautentisering, aksesskontroll, og integritet i systemene.
Normalt så holder de seg til de internasjonale normer og standarder
SIL- nivåer definert i EN50128
Lov, forskrifter, Europanormer
Datasikkerhet (brannmur, inntrenging etc.) i tillegg til oppetidskrav

Tabell 15: Bruker/kjøper/samarbeidspartneres krav til sikkerhet i programmerbare systemer

3.4.2 Utarbeidelse og oppfølging av sikkerhetskrav

I dette kapitlet fokuseres det på sikkerhetskrav, dvs. hva som gjøres innen bedriften for å forsikre seg om at systemene tilfredsstiller krav til sikkerhet.

Ni av bedriftene har kvalitetsikringsrutiner som fokuserer på programvarepålitelighet/ sikkerhet. Andre svar er :

- ingen offisiell standard (som ISO), følger egne rutiner
- delvis
- under innføring,

mens resten av svarene er benektende eller irrelevant. Det er også nevnt spesielle regler for modifikasjoner på sikkerhetssystemer, samt bruk av HAZOP analyser ved større modifikasjoner hvor man bl.a. ser på konsekvenser av at systemer feiler.

Høyt prioritert ved f.eks. å involvere eksterne institutter til å validere og verifisere våre konstruerte sikkerhets-løsninger
Egen sikkerhets-styring ble formalisert 01.01.01. All utvikling etter dette er underlagt ”sikkerhetshåndboka”
HMS styring, ikke spesielt på sikkerhet av programmerbare systemer
Adgangsbegrensning
Alle sikkerhetskritiske leveranser verifiseres internt av gruppen.
Noen ganger brukes en uavhengig 3. part som TüV, Sintef, DNV
Sikkerhetsvurderinger foretas fortløpende i prosessen i h t bestemmelser om produktutvikling
Adgangsbegrensning
Gjennom instruksverket. Også organisatorisk der det er en veldefinert vei til ledergruppa i større prosjekter

Tabell 16: I hvilken grad utvikling av sikkerhetskritiske systemer er underlagt bedriftens sikkerhetsstyring

En oversikt over i hvilken grad utviklingen av sikkerhetskritiske systemer er underlagt bedriftens sikkerhetsstyring er gitt i Tabell 16. Dette gjøres ofte i samarbeid med en kunde. Det blir også nevnt at MIL-882D setter krav om sannsynlighet vs. konsekvens. Se ellers Tabell 30 i appendiks B.

Åtte av disse igjen svarer klart positivt på om det utarbeides en samsvarsvurdering i henhold til gitte sikkerhetskrav, mens resten av svarene er benektende eller irrelevant (se Tabell 31 i appendiks B). Noen utfyllende svar er:

- Samsvar mot maskindirektiv, klassekrav + samsvar med spesifikasjon
- Systemer for nedstenging av B&G deteksjon verifiseres og sertifiseres av TüV ihht. IEC61508.
- Mot MIL-882D
- I noen tilfeller. Berøringsfare f.eks.

På spørsmålet om bedriften har dedikerte personer som er sikkerhetsansvarlig svarer åtte positivt (se Tabell 32 i appendiks B). Noen utfyllende svar er:

- Ja på én av systemtypene, noen ganger på andre produkter/prosjekter
- Hver enhet har en sikkerhetsleder. Når det gjelder sikkerhetssystemene har vi definert et systemansvar som er tillagt operasjonssjef, men hvor daglig arbeid er tillagt navngitt person
- Ja, i alle større prosjekter
- Ja, det finnes overordnet kvalitetssikringssystem, men ikke detaljert som antatt i 61508

De fleste bedriftene gjennomfører pålitelighets/risiko-analyser av kritiske systemer (se Tabell 33 i appendiks B). Noen utfyllende svar er:

- Komponentene gjennomgår FMEA og MIL217E beregning. Kritiske deler beregnes særskilt
- Det gjøres FMEA og kalkulasjoner av standard produktløsninger
- Det gjøres FMEA og kalkulasjoner av standard leverte systemer

Følgende spørsmål ble spesielt rettet til *produsenter* av kritiske systemer:

- Mener dere at deres programmer kan inngå i et sikkerhetskritisk system?
- Vil dere kunne få rettslig ansvar hvis programmet medfører en ulykke?
- Hvilke prinsipper anvendes i relasjon til risiko/pålitelighet (ALARP, kvantifiserte mål, inkrementelle forbedringer,)?

Detaljsvar er gitt i Tabell 34 i appendiks B.

Svarene fra de to første spørsmålene viser at de fleste produsentene mener at deres systemer kan anvendes i sikkerhetskritiske applikasjoner, og at de vedstår seg ansvarsforpliktelse hvis programmet medfører en ulykke. På spørsmålet om de ville kunne få rettslig ansvar hvis programmet/systemet

medfører en ulykke svarer 6 bedrifter ubetinget ja, 2 et betinget ja, mens en bedrift bruker klausul i kontrakter som begrenser ansvaret. Det nevnes spesielt at produktansvarsloven spesielt er viktig ved leveranser til USA. Det siste spørsmålet er uklart formulert, og svarene lite relevante.

Følgende spørsmål ble spesielt rettet til *brukerne*:

- I hvilken grad fokuserer dere på de spesielle utfordringene som gjelder for sikkerhet i programmerbare systemer?
- Har brukerne fått opplæring i de farer og risiko knyttet til bruken av systemer?

Detaljsvar er gitt i appendiks Tabell 35 i appendiks B.

Brukerbedriftene fokuserer på de spesielle utfordringene som gjelder for sikkerhet i programmerbare systemer. Derimot er svarene mer blandet når det gjelder opplæring om risikoaspekter ved bruk av systemene. En må, imidlertid, her ta i betraktning at bare fire rene brukerbedrifter har svart.

3.4.3 Krav til system for eventuell granskning i etterkant av en ulykke

Etter en ulykke vil det i de fleste tilfelle foretas en granskning av hva som var årsaken til ulykken, og hva som vil kunne gjøres for å hindre liknende ulykker i framtida. Spørsmålene i dette avsnittet er relatert til det, og svarene er gitt i Tabell 36, med et sammendrag i Tabell 17.

	Vil det være mulig å spore tilbake hvordan det programmerbare systemet fungerte før og under hendelsen?	**Vil det være relevant å logge systemtilstanden og funksjoner på tilsvarende måte som man gjør i et fly (blackbox)?**
ja	6	8
delvis	4	2
nei	2	1
irrelevant	2	1

Tabell 17: Oversikt over svar til spørsmål om sporbarhet

Den praktiske gjennomføringen av dette varierer, som en kunne forvente, mellom de forskjellige bedriftene:

- Funksjonen brukes i normal operasjon i dag på de systemene som er dekket
- Logging av definerte systemvariabler ved endring og hvert sekund
- Systemer som har vært involvert i en ulykke blir umiddelbart plombert av politiet
- Logging til historiestasjoner

- Det gjennomføres datalogging av våpensystemer ved bruk i fredstid (militærøvelser etc.)
- Event logging med en protokoll som ikke kan slettes
- Dette skal være mulig i de fleste store og moderne driftskontrollsystemer som energibransjen benytter i dag
- Felt analyse med kompetent personell, samt analyse av utskiftede komponenter

3.5 Behov for kompetanseheving og forskning

I dette kapittelet beskrives resultatene fra de spørsmålene som omhandler kompetansesituasjonen i dag, og de behov for kompetanseheving bedriftene selv har identifisert.

3.5.1 Kompetanse og kompetanseheving

Ni av bedriftene har hel eller delvis spesialkompetanse innen bedriften når det gjelder utvikling av kritisk programvare, mens 12 av dem supplerer med innleide konsulenter. Se detaljer i Tabell 37 i appendiks B.

Spesiell kompetanse?		**Konsulenter?**
Svar	**Antall**	**Antall**
Ja	5	12
Nei	2	2
Delvis	4	
Ikke relevant	3	
Totalt	**14**	**14**

Tabell 18: Oppsummering av tilgjengelig spesialkompetanse og bruk av konsulenter

Utviklingsfase	**Antall**
Kravspesifikasjon	9
Design	6
Utvikling	3
Produksjon	2
Testing	7
Operasjon	3
Modifikasjon	5

Tabell 19: Oversikt over de utviklingsfaser der bedriftene mener kompetansen bør styrkes

Tabell 19 gir en oversikt, basert på Tabell 39 i appendiks B, over de utviklingsfaser der bedriftene mener kompetansen bør styrkes. Det kommer klart fram fra denne tabellen at bedriftene ønsker å øke sin kompetanse for alle faser i utviklingen av kritiske programmerbare systemer.

Kravspesifikasjonen er klart det området der behovet for styrking av kompetanse er størst, mens produksjon, utvikling og operasjon kommer i den andre enden. Dette avspeiler kanskje at det er disse siste områdene bedriftene har satset mest på, eller at kravspesifikasjonen er den viktigste og vanskeligste fasen, den som krever mest kompetanse for å utføres tilfredsstillende.

Svarene på spørsmålet hvordan kompetansen når det gjelder sikker og pålitelig programvare bør utvikles er gitt i Tabell 40, og et sammendrag er gitt i Tabell 20. Svarene viser at spesialutdanning av sikkerhetsansvarlige og kursvirksomhet er de mest anbefalte metodene for kompetansestyrking innen bedriften, mens utdanningstilbud er viktigst i Norge generelt. Tatt i betraktning at det pr. i dag ikke finnes norske tilbud om spesialisering innen utvikling av kritiske programmerbare systemer er det åpenbart at slike tilbud bør etableres så snart som mulig.

Innen bedriften	**Antall**
Spesialutdanning av sikkerhetsansvarlige	10
Kursvirksomhet	8
Innleie av konsulenter	4
Nyansettelser	4
Selvopplæring, ”On the job training”	2

I Norge generelt	**Antall**
Utdanningstilbud	8
Internasjonalt samarbeid	6
Forskningsaktiviteter	6
Andre svar/kommentarer.	7

Tabell 20: Antall svar innen hver kategori om kompetanseutvikling

3.5.2 Behov for forskning og utvikling (FoU) i Norge

Spørsmålene her gjelder hvilke problemstillinger som bør tas opp i framtidig norsk forskning innen sikre og pålitelige programmerbare systemer, og svarene er (se Tabell 41 i appendiks B):

- Sikkerhetsmekanismer og sporbarhet
- Metodikk for verifikasjon/ validering av systemleveranser innenfor jernbanevirksomhet
- Primært på kravspesifikasjon, må lage enklere systemer som er lettere å operere og vedlikeholde
- Dokumentasjon for drift og vedlikehold. Spesifikasjon av sikkerhetssystemer
- Bruk av universelle produkter i stedet for spesialutviklede

- Gjenbruk, tillempe egnet utviklingsmetodikk, skalerbar prosess (etter sikkerhetskrav), estimering av utviklingsarbeid, bli flinkere til å fokusere på de viktige ting
- Modifikasjon og vedlikehold

På spørsmålet: Kunne dere tenke dere å delta i et slikt prosjekt?, fikk de tre svaralternativene følgende svar:

- indre kjerne 9
- ytre referansegruppe 5

En generell observasjon er at ikke alle bedriftene hadde klare meninger om hvilke problemstillinger de synes er viktigst. Imidlertid uttrykker alle at de er interessert i å være med i et slikt prosjekt, enten i en indre kjerne eller i en ytre referansegruppe. De fleste er i prinsippet interessert i å delta i en indre kjerne. At såpass få svarte at de ville delta med egeninnsats kan komme av at spørsmålet var uklart formulert.

4 Observasjoner og konklusjoner

Formålet med dette kartleggingsprosjektet har vært å undersøke aspekter som

- bruk
- utvikling
- sikkerhet
- kompetansebehov

når det gjelder kritiske programmerbare systemer

4.1 Kvaliteten på spørreskjemaet

For å oppnå dette ble det laget et spørreskjema som ble sendt ut til et sett av norske bedrifter. 14 av disse besvarte spørsmålene. For å komme med konklusjoner og forslag til videre innsats er det noen aspekter som må belyses.

- *Hvor representative er bedriftene som besvarte spørsmålene?*

De bedriftene som har besvart spørreskjemaet dekker et vidt spektrum, både når det gjelder rollekategori, marked og størrelse. Det er også en stor spredning i typer av systemer. Selv om utvalget ikke er stort er det rimelig å tro at de fleste bedrifter innenfor samme rolle/marked opplever situasjonen på samme måte.

- *Hvor relevante er spørsmålene?*

Formålet med spørrelista var å dekke et stort antall aspekter, for å sikre at flest mulig relevante opplysninger kom fram i svarene. Det er mulig, uten at vi positivt vet det, at størrelsen på spørrelista kunne virke skremmende på de som ikke svarte, og at vi med en mindre liste kunne fått flere svar. Dette var imidlertid en avveining som måtte gjøres.

- *Hvor gode er spørsmålene?*

Et annet problem er i hvilken grad spørsmålene var forståelige, og ble forstått likt, av bedriftene. Det var i den forbindelse nyttig at en del av spørrelistene ble besvart gjennom intervjuer. Det er imidlertid grunn til å tro at ikke alle spørsmålene ble oppfattet likt, men dette er i stor grad avklart gjennom svarene, slik at disse allikevel utgjør en god basis for å gjøre generelle konklusjoner.

I flere tilfeller er det klart at terminologien burde vært klarere definert. Spesielt gjelder dette begrepene sikkerhet, kritisk og sikkerhetskritisk, da det kan være tvil om disse begrepene er forstått likt av alle. Videre burde forskjellen mellom standard og utviklingsmetodikk vært klarere presisert i spørsmål der dette er relevant. Verifikasjon, validering og testing burde også vært definert, men det synes ikke som dette har vært noe problem for svarerne.

Som nevnt ovenfor ble spørrelista laget med henblikk på å dekke så mange aspekter som mulig i forbindelse med kritisk programvare. I ettertid, på

bakgrunn av analysen, kan det være naturlig å vurdere om spørrelista burde vært laget annerledes. For eksempel om en på forhånd hadde stilt opp klarere mål på hva en ønsket å få svar på ved undersøkelsen, og så konsentrere spørsmålene på disse målene.

Det må understrekes at dette er en overordnet kartlegging, og at det ville ha vært nødvendig med en langt mer spesifisert, og dermed vesentlig mer ressurskrevende, undersøkelse dersom det var ønsket å få mer detaljerte svar.

4.2 Observasjoner

Dette kapitlet gjengir de observasjonene som er gjort på basis av svarene, slik de er beskrevet i kapittel 3.

- *Beskrivelse av de utvalgte bedriftene*

Noen bedrifter dekker flere markeder, mens noen konsentrerer seg om ett enkelt markedssegment. Imidlertid er alle de foreslåtte markedene, med unntak av medisinsk utstyr, dekket av minst én bedrift. En konklusjon på dette kapitlet er at de bedriftene som har besvart spørreskjemaet dekker et vidt spektrum, både når det gjelder rollekategori, marked og størrelse.

- *Konsekvenser av feil*

11 av de 14 nevner tap av menneskeliv som (verst) mulig konsekvens. Det varierer mellom katastrofale følger (stort antall dødsfall) til enkeltpersoners skader, eventuelt død. Når det gjelder spørsmålet om det virkelig har skjedd ulykkeshendelser relatert til feilfunksjon av systemer kan svaret sammenfattes til: Ingen alvorlige, men muligens noen mindre hendelser.

Åtte nevner miljøskader, uten at de blir presentert nærmere. Alle nevner mulige økonomiske konsekvenser, noe som er naturlig for et system i aktivt bruk. Størrelsen varierer imidlertid stort, fra ca. 200 MNOK til manglende tilgjengelighet av systemet, og tap av tillit blant kunder.

- *Utvikling*

De fleste utviklere (systemprodusenter og hyllevareprodusenter) bruker standarder som grunnlag for programvareutvikling. Imidlertid brukes forskjellige standarder, både internasjonale standarder og bedriftsspesifikke standarder. Når det gjelder utviklingsmetodikk er svarene mer negative. Bare tre bedrifter nevner spesielle metoder.

Spørsmål om pålitelighetsmål og –data er bare relevante for utviklere av kritisk programvare. Fem av bedriftene svarte klart ja, men spørsmålet kan være uklart, dvs. om pålitelighetsmålene også omfatter programvaren. Når det gjelder pålitelighetsdata for programvare vil dette innebære en logging, med en detaljert beskrivelse, av programfeil som er oppdaget, og eventuelt rettet. Disse aspektene burde klargjøres bedre.

Alle bedriftene foretar noen form for verifikasjon og validering av sine produkter. Svarene gir imidlertid ikke mange detaljer på hvordan det gjøres, og ingen nevner verktøy som brukes. Om dette betyr at de ikke bruker hjelpeverktøy er uklart.

Når det gjelder teststrategi kan bedriftene deles i to grupper, de som planlegger testen fra begynnelsen, basert på funksjonsspesifikasjoner, og de som lager testprosedyrene på et seint stadium, rett før testen skal utføres. Det ville være interessant å sammenlikne erfaringer mellom disse framgangsmåtene.

- *Bruk*

Fra Tabell 5 ser en at kritiske programmerbare systemer har en bred anvendelse. Dette indikerer at det er behov for generelle prinsipper på dette området, som er anvendbare på mange typer systemer. Brukere av innkjøpt programvare setter generelt krav til kvalitetssikring hos produsenter/leverandører. Det virker imidlertid som forskjellige bedrifter bruker forskjellige standarder for disse kravene, men det er mulig at de underliggende prinsippene ikke er så forskjellige. Dette bør undersøkes videre, og også om det er behov for mer koordinering mellom bedrifter/bransjer.

Svarene på spørsmålene i avsnitt 0 indikerer at brukerbedriftene alle har gode rutiner for drift og vedlikehold. Dette inkluderer også rapportering av problemer. Det siste kan være av betydning hvis en ønsker å lage en problemdatabase for programvare.

- *Sikkerhet*

Sikkerhet ved bruk av programmerbare systemer var et vesentlig aspekt ved kartleggingen. Derfor var også mange av spørsmålene fokusert på dette. Dette gjelder både hvilke sikkerhetskrav som stilles, og hva bedriftene gjør for å oppfylle disse kravene.

Inntrykket fra svarene er at det stilles generelle sikkerhetskrav til kritiske systemer, men i mindre grad stilles spesielle sikkerhetskrav til programvare i slike system. Dette reflekterer det syn at det er systemer som sådan, og ikke programvaren i disse systemene som vil være en potensiell sikkerhetsrisiko. Dette gjelder både myndighetskrav og krav fra bruker/kjøper/samarbeidspartnere.

På spørsmålet om spesielle krav til sikkerheten i de programmerbare systemene, var svarene her, som når det gjelder myndighetskrav, at det enten ikke er noen slike spesielle krav, eller at de generelle krav skal følges. FAT og SAT tester blir nevnt. Det blir imidlertid påpekt at en forventer mer spesifikke krav i framtida.

På spørsmål om de ville kunne få rettslig ansvar hvis programmet medfører en ulykke svarer 6 bedrifter ubetinget ja, 2 et betinget ja, mens en bedrift bruker klausul i kontrakter som begrenser ansvaret.

- *Utarbeidelse og oppfølging av sikkerhetskrav*

Ni av bedriftene har kvalitetsikringsrutiner som fokuserer på programvarepålitelighet/ sikkerhet. Andre svar er :

- ingen offisiell standard (som ISO). følger egne rutiner
- delvis
- under innføring,

mens resten av svarene er benektende eller irrelevant

I hvilken grad utviklinga av sikkerhetskritiske systemer er underlagt bedriftens sikkerhetsstyring varierer en del mellom bedriftene. Seks av bedriftene har klare rutiner for sikkerhetsstyring.

Andre svar er:

- HMS styring, ikke spesielt på sikkerhet av programmerbare systemer
- Adgangsbegrensning
- I tilstrekkelig grad,

mens resten av svarene er benektende eller irrelevant

Tolv av bedriftene svarer positivt på at de utarbeider sikkerhets- og pålitelighetskrav til sikkerhetskritiske system, basert på risikoanalyser og behov for risikostyring og risikoreduserende tiltak. Dette gjøres ofte i samarbeid med en kunde.

Åtte av disse igjen svarer klart positivt på om det utarbeides en samsvarsvurdering i henhold til gitte sikkerhetskrav.
Andre svar er:

- I noen tilfeller, som f.eks. berøringsfare
- I 2001 er det gjennomført en total gjennomgang av teknisk tilstand på sikkerhetssystemene på samtlige anlegg i drift,

mens resten av svarene er benektende eller irrelevant

På spørsmålet om bedriften har en dedikert person som er sikkerhetsansvarlig svarer åtte positivt. Tre andre svar er imidlertid delvis positive, idet de ikke har én sikkerhetsansvarlig i bedriften, men sikkerhetsansvarlig i de enkelte prosjekter.

De fleste bedriftene gjennomfører pålitelighets/risiko-analyser av kritiske systemer.

De fleste produsentene mener at deres systemer kan anvendes i sikkerhetskritiske applikasjoner, og at de vedstår seg ansvarsforpliktelse hvis programmet medfører en ulykke. Det siste spørsmålet er uklart formulert, og svarene lite relevante.

Brukerbedriftene fokuserer på de spesielle utfordringene som gjelder for sikkerhet i programmerbare systemer. Derimot er svarene mer blandet når det gjelder opplæring om risikoaspekter ved bruk av systemene. En må, imidlertid, her ta i betraktning at bare fire rene brukerbedrifter har svart.

Etter en ulykke vil det i de fleste tilfelle foretas en granskning av hva som var årsaken til ulykken, og hva som vil kunne gjøres for å hindre liknende ulykker i framtida. 9 av 14 svarer mer eller mindre positivt på at det vil være mulig å spore tilbake hvordan det programmerbare systemet fungerte før og under hendelsen. For to av bedriftene er spørsmålet irrelevant, mens tre bedrifter svarer negativt. Tilsvarende positive er svarene til spørsmålet om muligheten logge systemtilstanden og funksjoner på tilsvarende måte som man gjør i et fly. Den praktiske gjennomføringen av dette varierer, som en kunne forvente, mellom de forskjellige bedriftene.

- *Behov for kompetanseheving og forskning.*

Ni av bedriftene har hel eller delvis spesialkompetanse inne bedriften når det gjelder utvikling av kritisk programvare, mens 12 av dem supplerer med innleide konsulenter.

Det kommer klart fram fra svarene at alle bedrifter ønsker å øke sin kompetanse for alle faser i utviklingen av kritiske programmerbare systemer. Kravspesifikasjonen er klart det området der behovet for styrking av kompetanse er størst, mens produksjon, utvikling og operasjon kommer i den andre enden. Dette avspeiler kanskje at det er disse siste områdene bedriftene har satset mest på, eller at kravspesifikasjonen er den viktigste og vanskeligste fasen, den som krever mest kompetanse for å utføres tilfredsstillende.

Svarene viser videre at spesialutdanning av sikkerhetsansvarlige og kursvirksomhet er de mest anbefalte metodene for kompetanse styrking innen bedriften, mens utdanningstilbud er viktigst i Norge generelt.

Når det gjelder framtidig forskning hadde ikke alle bedriftene klare meninger om hvilke problemstillinger de synes er viktigst. Imidlertid uttrykker alle at de er interessert i å være med i et slikt prosjekt, enten i en indre kjerne eller i en ytre referansegruppe. De fleste er i prinsippet interessert i å delta i en indre kjerne.

4.3 Generelle konklusjoner

Dette kartleggingsprosjektet har hatt som et formål å legge grunnlag for nye prosjekter innen produksjon og bruk av kritisk programvare, i samarbeid mellom industri, forsknings- og undervisningsinstitusjoner.

Selv om det er et begrenset antall besvarelser, kommer det klart fram at sikkerhetsaspektet ved bruk av digital teknikk er noe som blir tatt seriøst av norske bedrifter. Selv om de har egne rutiner i denne forbindelse, ønsker

imidlertid bedriftene generelt å øke kompetansen innen området. Dette gjelder alle aspekter, men med spesiell vekt på forbedring av kravspesifikasjonene.

Bedriftene nevner både utdanningstilbud, forskningsaktiviteter og samarbeid som måter for å heve kompetansen. I den forbindelsen uttrykker alle bedriftene at de er interessert i å være med i et eventuelt forskningsprosjekt innen sikre og pålitelige programmerbare systemer. I parallell med kartleggingsprosjektet er det derfor blitt utarbeidet et forslag til Norsk Forskningsråd om et konkret samarbeidsprosjekt mellom bedrifter og forskningsinstitusjoner.

Dette kartleggingsprosjektet har avdekket et behov for videre aktiviteter innen dette området i Norge. En forutsetning for dette er at det blir laget konkrete undervisningsplaner ved våre universiteter og høgskoler for å utdanne kompetente personer. Videre bør samarbeidet mellom bedrifter, forsknings- og undervisningsinstitusjoner styrkes, gjennom det eksisterende NONSTOPP-nettverket, ved seminarer, slik det som ble holdt i Halden i oktober 2000, og ved konkrete samarbeidsprosjekter. Siden bedriftene rapporterer et klart behov for kompetanseheving innen en rekke temaer relatert til utvikling av kritiske programmerbare systemer, bør det startes et flerårig forskningsprosjekt som dekker et stort spekter av problemstillinger. M.a.o bør et slikt prosjekt ha som formål å øke kunnskapen om hele utviklingsløpet. I tillegg vil dette også kunne skape et grunnlag for en erfaringsdatabase som andre norske bedrifter og forsknings- og undervisningsinstitusjoner vil kunne nyttiggjøre.

5 Forslag til forskningstemaer for videre FoU-innsats

Som nevnt tidligere har en hensikt med denne kartleggingen vært å skape et grunnlag for å definere konkrete forskningsprosjekter innen dette fagområdet. Når man skal forsøke å trekke ut spesielle temaer og anbefale disse for videre FoU-innsats, er det viktig å huske at denne kartleggingen har fokusert på bedrifter, dvs. miljøer som i stor grad er opptatt av de praktiske problemene med utvikling og bruk av kritiske programmerbare systemer. Dette betyr at de forskningstemaene som foreslås her i stor grad vil være av anvendt karakter. At det er et faktisk behov for mer FoU-innsats innen dette temaområdet er åpenbart når man ser bedriftenes svar når det gjelder behov for slike aktiviteter og villighet til å bidra. Hele 9 av de 14 bedriftene ønsket å delta i en indre kjerne i et FoU-prosjekt, noe som kanskje mer enn noe annet forteller at disse bedriftene har reelle behov.

5.1 Utarbeidelse av krav, spesielt sikkerhetskrav

På spørsmålet om hvilke faser i utviklingen bedriftene hadde størst behov for forbedring var det kravfasen som klarest fremsto som et problemområde. Mange bedrifter føler seg usikre på hvordan man best gjennomfører denne fasen.

- Kravfasen er svært viktig siden den legger premissene for hvilket system som til slutt blir implementert.
- Identifikasjon, spesifisering og verifikasjon av sikkerhetskrav er essensielt for å oppnå nødvendig sikkerhetsnivå. Bestemmelse av SIL-nivåer er en del av dette, men i denne forbindelse bør fokuset være mer på å finne frem til hvilke egenskaper som må bygges inn i systemet for å oppnå sikkerhet.

5.2 Tilpassing av utviklingsmetodikk for utvikling av kritisk programvare

Svarene på spørsmålene relatert til utviklingsmetodikk var ganske divergerende, og tyder på at dette er et område det er ønskelig med mer kunnskap, og et behov for generelt aksepterte metoder for hvordan utvikling av kritisk programvare faktisk bør foregå.

- Eksplisitte krav om at programmerbare systemer må utvikles i henhold til spesifikke sikkerhetsstandarder er for mange bransjer relativt nytt.
- Mens de fleste sikkerhetsstandarder tar utgangspunkt i tradisjonelle sekvensielle utviklingsløp, har det de siste årene i mange miljøer vært en overgang til eksplisitte iterative utviklingsløp. Det er derfor viktig at disse utviklingsløpene både evalueres og eventuelt justeres slik at de blir egnet til bruk ved utvikling av kritisk programvare.

- Tradisjonelt har utviklingsløp og risikohåndtering ikke vært spesielt nært koordinert. I forbindelse med de nye utviklingsmetodikkene vil det være nødvendig å kople risikohåndtering og utvikling mye tettere dersom man skal kunne oppfylle kravene i standardene.
- Det finnes allerede teoretiske arbeider fra både Høgskolen i Østfold og NTNU som fokuserer på denne problemstillingen og som kan brukes som utgangspunkt for bedriftsprosjekter.

5.3 Utarbeidelse av anbefalinger vedrørende gjenbruk av pre-eksisterende programvare

Gjenbruk av programvare kan skje ved at en bruker om igjen programvare som er utviklet til annet formål, eller at en bruker standard, kommersielt tilgjengelige, programmer. Undersøkelsen viste tydelig at det blant bedriftene var stor sprik i hvordan man håndterer innkjøpt programvare, og det er rimelig å tro at det ved håndtering av alle typer gjenbruk av programvare mangler gode rutiner.

- Svært få standarder sier noe om dette, og de som gjør det gir kun overordnede retningslinjer.
- Gjenbruk har blitt et viktig tema innenfor alle typer programvareutvikling og er derfor også et tema det forskes mye på internasjonalt, men hvor det er en del som gjenstår før man kan gi detaljerte og gode råd om hvordan dette bør håndteres i kritiske systemer.
- Det er ønskelig med metoder for hvordan en skal ta hensyn til tidligere erfaring og annen relevant informasjon om kommersielt tilgjengelige programvareprodukter når en skal vurdere om de kan brukes i sikkerhetskritiske systemer.

5.4 Verifikasjon/validering

På spørsmål relatert til verifikasjon/validering og testing var det sprikende svar på valg av strategier. Det er i den forbindelse flere aspekter som kan undersøkes.

- Hvilke erfaringer er gjort med forskjellige strategier, f.eks. når det gjelder statisk analyse eller testing.
- Hvilke konsekvenser har det om testplaner utarbeides tidlig eller seint i utviklingsløpet.
- Hvilke bidrag gir forskjellige teststrategier (”black box”, ”white box”, statistisk testing, etc.) til etableringen av et sikkerhetsargument (”safety case”)

5.5 Sammenligning av standarder

Siden de kartlagte bedriftene representerer forskjellige markeder henviser de også til forskjellige standarder som relevante for sitt arbeide.

- Sikkerhet i programmerbare systemer er grunnleggende sett det samme problemet uansett anvendelsesområde og det ville vært interessant å sammenlignet forskjellige standarder for å kartlegge likheter og forskjeller.
- En slik oversikt ville gjøre det langt lettere å planlegge og gjennomføre forskningsprosjekter på tvers av bransjer i fremtiden.

5.6 Etablering av en sentral database for feil i kritiske programmerbare systemer

Selv om de kartlagte bedriftene synes å ha gode rutiner for drift av kritiske systemer er det i dag vanskelig å få tilgang på de erfaringene som gjøres for bruk i fremtidige utviklingsprosjekter. Det ville derfor være verdifullt dersom det kunne la seg gjøre å etablere en sentral database for observerte feilhendelser i kritiske programmerbare systemer.

- Etableringen av en slik database ville være et instrument for kunnskapsoverføring mellom bransjer.
- Fordi en økende andel av systemene er basert på standardkomponenter vil en slik database gi bedre muligheter til å vurdere om konkrete programvareprodukter er egnet for bruk i kritisk sammenheng eller ikke.

Appendiks A Det utsendte spørreskjemaet

Følgende spørreskjema ble sendt til bedriftene (sammen med en innledning som ikke er tatt med her)

Kartlegging

Organisasjon/aktør, kontaktperson, adresse, telefon,....

Rolle

Hvilken rolle har bedriften i forhold til programmerbare sikkerhetskritiske systemer.

1. Designer
2. Produsent
3. Bruker/operatør
4. Entreprenør/integrator (en som setter sammen og leverer programmerbare systemer basert på innkjøpte komponenter
5. Vedlikeholder
6. Tilsynsmyndighet
7. Konsulent, 3. parts verifikasjon, sertifisering
8. Annet

Marked

Hvilke marked(er) er bedriftens hovedområde?

1. Olje/gass
2. Energiproduksjon/energiforsyning
3. Luftfart/romfart
4. Skipsfart
5. Tog
6. Veitransport
7. Prosessindustri
8. Telecom
9. Data/informasjonsbehandling
10. Internett relatert tjeneste tilbyder
11. Forsvar
12. Produsent av utviklings/analyseverktøy (software og/eller hardware)
13. Farmasøytisk industri
14. Medisinsk utstyr
15. Annet?

Størrelse

Hva er bedriftens størrelse i antall årsverk i Norge?
Hvor mange av disse er relatert til utvikling eller bruk av kritiske programmerbare systemer?

Funksjon/anvendelse

Hvilke type funksjoner utøves av de sikkerhetskritiske systemene?
(eks: deteksjon, nedstengning, kontroll/prosesstyring, bremsesystem, signalsystem,....)

Hvilken type konsekvens har feil av systemene?

1. Tap av menneskers liv eller helse
2. Skade på miljø
3. Tap av økonomiske verdier eller anseelse

Hvor store konsekvenser kan i verste tilfelle oppstå for sluttbruker/operatør ved feil av systemene per ulykkeshendelse?

Hvor mange systemer er i bruk i Norge fra din bedrift i dag?

Hvor mange ulykkeshendelser relatert til feilfunksjon av system kjenner man til?

Sikkerhetskrav

Stiller myndighetene krav til sikkerhet?
Hvis ja, hvilke krav?
Svar:

Stiller myndighetene spesielle krav til sikkerheten i de programmerbare systemene?
Hvis ja, hvilke krav?
Svar:

Stiller bruker/kjøper/samarbeidspartnere krav til sikkerhet?
Hvis ja, hvilke krav?
Svar:

Stiller bruker/kjøper/samarbeidspartnere spesielle krav til sikkerheten i de programmerbare systemene?
Hvis ja, hvilke krav?
Svar:

Utarbeidelse og oppfølging av sikkerhetskrav.
Hva gjøres innen bedriften for å forsikre seg om at systemene tilfredsstiller krav til sikkerhet.

1. Har dere kvalitetsikringsrutiner som fokuserer på programvarepålitelighet/ sikkerhet?
   Svar:
2. I hvilken grad er utvikling av sikkerhetskritiske systemer underlagt bedriftens sikkerhets-styring?
   Svar:
3. Utarbeides det sikkerhets og pålitelighetskrav til sikkerhetskritiske system?
   Svar:
4. Baseres slike krav på risikoanalyser og behov for risikostyring og risikoreduserende tiltak?
   Svar:
5. Utarbeides det en samsvarsvurdering i henhold til gitte sikkerhetskrav? (ihht forskrift elektromedisinsk utstyr, produktansvarsloven, IEC 61508 Functional Safety Assessment,...)
   Svar:
6. Har dere en dedikert person som er sikkerhetsansvarlig?
   Svar:
7. Har noen av personene som er involvert i utviklingen spesiell kompetanse når det gjelder utvikling av kritisk programvare?
   Svar:
8. Henter dere inn sikkerhetskompetanse fra eksterne leverandører/konsulenter?
   Svar:
9. Hvilken kompetanse har dere når det gjelder utvikling av kritiske programmerbare systemer?
   a. Utviklingsmetodikk?
   b. Risikoanalyser?
   c. Verifikasjon/validering/samsvarsvurdering
   d. Annet?

   Svar:
10. Har dere behov for å øke kompetansen på disse områdene eller andre områder relatert til sikkerhet?
    Svar:

11. I hvilken utviklingsfase trenger man mest å styrke kompetansen (kravspek, design, utvikling, produksjon, testing, operasjon, modifikasjon)?
    Svar:

Kompetanseoppbygging

Hvordan bør kompetansen når det gjelder sikker og pålitelig programvare utvikles?

1. Innen bedriften:
    a. Kursvirksomhet?
    b. Spesialutdanning av sikkerhetsansvarlige?
    c. Nyansettelser?
    d. Innleie av konsulenter?

   Svar:
2. I Norge generelt:
    e. Utdanningstilbud ved universitet og høgskoler?
    f. Forskningsaktiviteter?
    g. Internasjonalt samarbeid?

   Svar:

Krav til system fra granskningskommisjon i etterkant av en mulig ulykke

Gitt at det har skjedd en utilsiktet hendelse eller en alvorlig ulykke og at det gjennomføres en granskning av hendelsesforløpet. Det vil være av interesse å søke etter informasjon i det programmerbare sikkerhetskritiske systemet.

1. Vil det være mulig å spore tilbake hvordan det programmerbare sikkerhetskritiske systemet fungerte (feilfunksjon) før og under hendelsen?
Svar:

2. Vil det være relevant å logge systemtilstanden og funksjoner på tilsvarende måte som man gjør i et fly (blackbox)?
Svar:

3. Hva er praksis (state of the art) for de produkter som bedriften er relatert til?
Svar:

Behov for forskning og utvikling (FoU) i Norge?

Hvilke problemstillinger synes dere at man bør fokusere på i et eventuelt fremtidig forskningsprosjekt innen feltet ”Utvikling av kritiske programmerbare systemer”?
Svar:

Kunne dere tenke dere å delta i et slikt prosjekt?

1. Ja, i en indre kjerne (delta med forpliktende innsats i NFR søknad)
2. Ja, i en ytre referansegruppe.
3. Nei.

Svar:

Spesielle spørsmål til forskjellige typer av aktører

Hyllevareprodusenter (dvs. systemer som selges på det åpne marked)

1 Baserer dere utviklingen på noen spesifikk standard? Hvis ja, hvilken?
Svar:

2 Brukes det noen spesiell utviklingsmetodikk? Hvis ja, hvilken?
Svar:

3 Brukes det en spesiell utviklingsmetodikk i forhold til sikkerhet?
Svar:

4 Foretas noen verifikasjon og/eller validering av programmene i forhold til sikkerhet? I tilfelle, hvordan? Hvilke verktøy?
Svar:

5 Settes det mål for pålitelighet?
Svar:

6 Vil dere på spørsmål kunne produsere pålitelighetsdata?
Svar:

7 Mener dere at deres programmer kan inngå i et sikkerhetskritisk system?
Svar:

8 Vil dere kunne få rettslig ansvar hvis programmet medfører en ulykke?
Svar:

Systemprodusenter*:*
(som leverer programmerbare systemer. Inkluderer både de som leverer skreddersydd programvare og de som setter sammen eksisterende komponenter)
Hvilke krav stiller dere til leverandør av programvaren?

1. Erfaring
2. Utviklingsmetodikk
3. Utviklingsmetodikk i forhold til sikkerhet
4. Kvalitetssikring
5. Tidligere leveranser av programmer i sikkerhetskritisk anvendelse

6. Annet?

Svar:

Hvilke krav stiller dere til innkjøpt programvare?

1. Programdokumentasjon
2. Oppfylling av standarder
3. Verifikasjon/testing
4. Dokumentasjon av relevante data
    a. versjonshistorie
    b. logging av feildata
    c. brukererfaring

Svar:

I hvilken grad fokuserer dere på de spesielle utfordringene som gjelder for utvikling av sikker og pålitelig programvare?

1 Baserer dere utviklingen på noen spesifikk standard? Hvis ja, hvilken?
Svar:

2 Brukes det noen spesiell utviklingsmetodikk? Hvis ja, hvilken?
Svar:

3 Når skrives testprosedyrene og gjennomføres testing etter en testplan
Svar:

4 Foretas noen verifikasjon og/eller validering av programmene?
    a. I tilfelle, hvordan? Hvilke verktøy?
    b. Er det krav til verifikasjon/validering av uavhengig organisasjon/3. part?

Svar:

5 Settes det mål for pålitelighet?
Svar:

6 I hvilken grad gjøres det risiko og pålitelighetsanalyser av systemene?
Svar:

7 Hvilke prinsipper anvendes i relasjon til risiko/pålitelighet (ALARP, kvantifiserte mål, inkrementelle forbedringer,...)?
Svar:

8 Vil dere på spørsmål kunne produsere pålitelighetsdata?
Svar:

9 Mener dere at deres programmer kan inngå i et sikkerhetskritisk system?
Svar:

10 Vil dere kunne få rettslig ansvar hvis programmet medfører en ulykke?
Svar:

Brukere som anvender sikkerhetskritiske systemer

1. Hvilke krav stiller dere til leverandør av de programmerbare systemene?

Svar:

2. I hvilken grad fokuserer dere på de spesielle utfordringene som gjelder for sikkerhet i programmerbare systemer?
   Svar:
3. Gjennomfører dere risikoanalyser i forbindelse med etablering og idriftsettelse?
   Svar:
4. Har brukerne fått opplæring i de farer og risiko knyttet til bruken av systemer?
   Svar:
5. Har brukerne kjennskap til forutsetninger for bruk av systemene?
   Svar:
6. Har brukerne fått opplæring i nødvendig oppfølgning mht behov for å identifisere nødvendig vedlikehold?
   Svar:
7. Logges og rapporteres faresituasjoner under drift?
   Svar:
8. Logges driftsproblemer og erfaringer med systemer under drift?
   Svar:

Appendiks B Tabeller med faktiske svar

Av hensyn til konfidensialiteten er svarene til den enkelte bedrift listet i tilfeldig rekkefølge i hver tabell, for på denne måten å forhindre sporbarhet av de enkelte svarene.

Rolle	**Marked**
Designer Produsent Entreprenør/integrator Vedlikeholder Konsulent, 3. parts verifikasjon, sertifisering	Olje/gass Skipsfart Prosessindustri Farmasøytisk industri (Prosess og farmasi er mindre deler)
Designer Produsent Bruker/operatør Entreprenør Vedlikeholder	Tog
Designer Produsent Entreprenør/Integrator Vedlikeholder	Olje/gass
Designer Produsent Bruker/operatør Entreprenør/integrator Vedlikeholder	Telecom
Bruker/operatør Vedlikeholder	Olje/gass
Designer Produsent Bruker/operatør Entreprenør	Olje/gass Skipsfart
Designer Produsent	Bil industri og øvrig masseproduserende industri med høy grad av fleksibel automasjon
Designer Produsent Bruker/operatør Entreprenør Vedlikeholder	Luftfart/romfart Skipsfart (militær) Telecom Data/informasjonsbehandling Internett relatert tjeneste tilbyder (ikke mye) Forsvar Produsent av utviklings/analyseverktøy
Bruker/operatør	Energiproduksjon/forsyning
Designer Entreprenør/integrator Vedlikeholder	Olje/gass Tog Prosess
Designer	Olje/gass

Produsent Vedlikeholder	Skipsfart Forsvar
Konsulent, 3. parts verifikasjon, sertifisering	Tog
Designer Produsent Bruker/operatør Konsulent, 3. parts verifikasjon, sertifisering	Skipsfart Veitransport Prosessindustri (Maritimt, fiskematproduksjon).
Designer Produsent	Luftfart/romfart

Tabell 21: Roller og markeder for de enkelte bedriftene

Hva er bedriftens størrelse i antall årsverk i Norge?	**Hvor mange av disse er relatert til utvikling eller bruk av kritiske programmerbare systemer**
15000	26. Ca. 8 personer med et hovedfokus på sikkerhetssystemer, men alle 26 har en befatning med det
75	20
500	50
145	5
1000	ca. 800
900	500
750	20
4500	1000
3568	ca 20 - 30 % av de ansatte er i befatning med sikkerhetskritiske systemer på en eller annen måte
22	9
230	70
800	50
250	25
17	15

Tabell 22: Antall ansatte totalt og antall ansatte som utvikler eller bruker kritiske programmerbare systemer

Type system
Konfigurering av telenett, og faktura informasjon
kontroll/prosesstyring, operatørstøttesystem
Deteksjon, nedstengning, kontroll/prosesstyring, skipskontroll posisjonering
Robot systemer for anvendelse i masseproduserende industri som bilprodusenter
Våpenkontrollsystemer Våpenkommunikasjonssystemer Kontroll-programvare Luftfartsovervåking Romfart (ikke programvare)
Satellittnavigasjon, Bakkeradar, Talekommunikasjon for flygeledere
Kontroll/styring av sikkerhetssystemer
Kontroll / prosess, maskinstyring
Deteksjon, “nedstengning” (sette signaler i stopp), manøvrere/sperre aktuatorer, automatisk togstopp,

Kontroll/prosesstyring – inkl. vernstyring (regionalt strømnett)
Deteksjon, kontroll/prosesstyring, bremsesystem og signalsystem
Brann og gass deteksjon, Nedstengning, signalsystem
Hovedanvendelsene er B&G deteksjon, nødavstengning og prosess-nedstengning. Men også kommunikasjonssystemene anses som sikkerhetssystemer, fakkelsystemet, trykkavlastningssystemet, brannpumpekontroll, og sikkert andre.
Komponenter for posisjonering, attitude control

Tabell 23: Typer av systemer for hver bedrift

Hvilken type konsekvens har feil av systemene?	**Hvor store konsekvenser kan i verste tilfelle oppstå for sluttbruker/operatør ved feil av systemene per ulykkeshendelse?**	**Hvor mange systemer er i bruk i Norge fra din bedrift i dag?**	**Hvor mange ulykkeshendelser relatert til feilfunksjon av system kjenner man til?**
Menneskeliv/helse Miljøskade Økonomiske verdier, men faktiske hendelser har gitt tap av produksjon og miljøskadelige utslipp	-	IR	Faktiske hendelser har gitt tap av produksjon og miljøskadelige utslipp
Miljøskade Økonomiske verdier	Ingen sikkerhetskritiske konsekvenser, men produksjon av produkter med feil kvalitet (kan ha miljøkonsekvenser) økonomisk tap	10	ingen
Alle, avhengig av i hvilket system komponenten brukes	Komponentleverandør så det er utenfor deres kontroll	Opp mot 1000	Helikopter landet hardt. SW-feil. Algoritme-feil.
Menneskeliv/helse Miljøskade Økonomiske verdier	Mulig død for en eller flere personer Forurensning Store økonomiske for kunde	Landindustri og olje/gass: ca 30 fartøys-automasjon	-
Menneskeliv/helse Miljøskader Økonomiske verdier	ca 200 mnok, skade på liv og helse, miljø	1800	5
Menneskeliv/helse Miljøskader (indirekte) Økonomiske verdier	Tap av menneskeliv	konfidensielt	Ingen alvorlige. Muligens noen mindre hendelser
Menneskeliv/helse Økonomiske verdier	Titalls drepte + titalls skadde	IR	0
Menneskeliv/helse Miljøskade Økonomiske verdier	Tap av liv og tap av materiell (katastofe-aspektet)	100 (verdensbasis 40.000 (HIMA))	Ingen
Menneskeliv/helse Økonomiske verdier	Tap av menneskeliv	>100	1
Økonomiske verdier	Manglende tilgjengelighet	15	0
Økonomiske verdier	7	IR	?
Menneskeliv/helse Miljøskader Økonomiske verdier	: Katastrofale	ca. 300	ingen

Menneskeliv/helse Økonomiske verdier	Tap av 2-300 menneskeliv	ca. 100	ingen
Menneskeliv/helse* Økonomiske verdier * Robotcellene er avskjermet med forriglede sikkerhetsbarrierer/gjerder under produksjon, samt Live Handle safety under programmering (hardware løsning)	Produksjonsstans	2-300 roboter totalt (sveise og lakk roboter)	Person skader meget få. Skade av roboter (dvs. for eksempel kollisjon med periferi utstyr) som kan ha forårsaket produksjons stans er vanskelig å kvantifisere

Tabell 24: Oversikt over konsekvenser, alvorlighet av feil, utbredelse av systemene og kjente ulykkeshendelser

Settes det mål for pålitelighet?	**Vil dere på spørsmål kunne produsere pålitelighetsdata?**
ja	Data med en viss grad av pålitelighet kan produseres for enkelte systemer og komponenter
nei	Data om driftsstabilitet
Nei, bare kvalitative krav	I noen grad (måler oppetid på systemene fordi dette er grunnlag for fakturering)
ja	ja
Skulle gjerne hatt bedre logge-system, men det arbeides med det	ja
Ikke på programmer	Noe krav og analyse på sikkerhetsfunksjon som er gjennomført i designfasen. Finnes ikke data fra operativ fase
Krav fra kunder, men angir også feilfrekvens for komponenter (basert på HW)	Ja, men ikke enkelt. Har servicerapporter og god kontroll med software oppdateringer og fikses
Ja for visse systemer, sjeldent for andre	ja
ja	ja
ja	ja

Tabell 25: Pålitelighetsmål og pålitelighetsdata

Hvilke krav stiller dere til leverandør av programvaren?	**Hvilke krav stiller dere til innkjøpt programvare?**
Lager de fleste komponenter selv. Kan bli bedre til å stille krav til underleverandører	Oppfylling av standarder Verifikasjon/testing Dokumentasjon av relevante data (versjons-historie, logging av feildata, brukererfaring) (Forbedringspotensiale)
DNV sertifisert	NA, lager software selv
Kvalitetssikring av produktene fra leverandørene sjekkes	Programdokumentasjon.
Erfaring Utviklingsmetodikk Utviklingsmetodikk i forhold til sikkerhet Kvalitetssikring	alle
Erfaring Utviklingsmetodikk Utviklingsmetodikk i forhold til sikkerhet Kvalitetssikring Tidligere leveranser	Programdokumentasjon Oppfylling av standarder Verifikasjon/testing Dokumentasjon av relevante data (versjonshistorie, logging av feildata, brukererfaring)
Fortrinnsvis erfaring Utviklingsmetodikk i forhold til sikkerhet Kvalitetssikring Tidligere leveranser av programmer i sikkerhetskritisk anvendelse Sertifisert programvare er ofte en nødvendighet for å kunne verifisere totalpåliteligheten	Sertifisert software og oppfylling av standarder
At de i størst mulig grad følger standarder	-
Alt dette er av betydning. Leverandørene skal tilfredsstille samme krav som det stilles til KDA. Det er satt opp en ”Maturity Capability Model” som produsentene vurderes etter	MIL-882D Oppfylling av standarder Verifikasjon/testing
I fremtiden vil vi stille krav om SIL-klasse	-
Funksjonelle krav etter OPC-standarden Utvikler de kritiske komponentene selv	Oppfylling av OPC-standard Bruk av standard testing
De skal være forhåndsgodkjent i Sellihca	-
Varierende krav, Bruker ADA i navigasjon	ADA 3.80 godkjent standard
Relevante punkter i EN 61508, EN 50126, EN 50128, EN 50129	-
Erfaring med leverandør, kvalitetssikring	Lite relevant

Tabell 26:Krav til leverandører og innkjøpt programvare

Stiller myndighetene krav til sikkerhet?	**Stiller myndighetene spesielle krav til sikkerheten i de programmerbare systemene?**
Militære standarder (MIL 882D). Luftfartsverkets standarder for luftfartssystemer	Militære standarder (MIL 882D). DO-178B luftfartssystemer Redundans og sikkerhetsbarrierer. Ikke to barrierer på samme CPU
Oljedirektoratets regelverk gjelder	Oljedirektoratets regelverk gjelder
: De stiller personvernmessige krav	nei
Forskrift for elektriske anlegg - Forsyningsanlegg (FEA-F) Forskrift om sikkerhet ved arbeid i og drift av høyspenningsanlegg med veiledning (FSH) Forskrift om sikkerhet ved arbeid i og drift av lavspenningsanlegg (FSL) Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid (IK) Forskrift om elektrisk utstyr (FEU) Forskrift om kvalifikasjoner for elektrofagfolk med veiledning (FKE)	Beredskapshåndbok for kraftforsyningen" - kapittel 5 Sikkerhet, fastsatt av NVE, februar 1997. "Sikkerhetsbestemmelser for Kraftforsyningen", fastsatt ved kronprinsregentens res av 11. januar 1991. "Sikkerhetsinstruksen" med utfyllende bestemmelser og "Beskyttelsesinstruksen", fastsatt ved kgl. res. av 17. mars 1972, sist endret ved kgl. res. av 7. oktober 1988. "Direktiv for sikring av datasystemer gradert etter Sikkerhetsinstruksen eller Beskyttelsesinstruksen", gitt av Forsvarssjefen 28. januar 1998 ("Datasikkerhetsdirektivet")
EU direktiver Direktorater (olje, sjøfart) Produkt og Elektrisitetstilsynet	Ja - mange
Iht Jernbaneloven, inkl forskrifter	Enkeltfeil skal ikke føre til tap av menneskeliv eller alvorlig personskade
Ja, sokkelstatskrav	Nei, men det antas å komme krav
Jernbaneloven med tilhørende forskrifter, spesielt forskrift av 23.12.00	Jernbaneloven med tilhørende forskrifter, spesielt forskrift av 23.12.00.
Ja, Krav til barrierer iflg. Oljedirektoratets styringsforskrift. Den Nye Internasjonale Sikkerhetsstandarden IEC 61508 er introdusert gjennom OD-veiledning 070 (– OLF Guideline for IEC61508 og IEC 61511)	OD-veiledning 070 (– OLF Guideline for IEC61508 og IEC 61511). Flere krav vil fremtvinge seg.
Nei	nei
Ja for visse systemer	Ja for visse systemer.
Ja, OD krav, maskinforskriften, elektriske forskrifter	: Ikke myndighetskrav i dag, krav vil komme
Ennå ikke, men det kan komme EU-krav	nei
Ref. ISO og EN standarder mht sikkerhet og spesifikt for Roboter	Ref. ISO og EN standarder mht sikkerhet og spesifikt for Roboter

Tabell 27: Myndighetskrav til sikkerhet

Stiller bruker/kjøper/ samarbeidspartnere krav til sikkerhet?	**Stiller bruker/kjøper/samarbeidspartnere spesielle krav til sikkerheten i de programmerbare systemene?**
Bare overordnede krav	Bare overordnede krav
For det militære, se tabell 8. Andre kunder, som Lockhead Martin og Raytheon, bruker sine egne sikkerhetskrav. For romfart brukes ECSS-standarden.	Brukerne stiller stort sett generelle sikkerhetskrav, ikke spesifikt for programvare
nei	-
I noen tilfeller (romfart). Når det gjelder pålitelighet og tilgjengelighet så har flere kunder krav	Vanlig med FAT og SAT
nei	De stiller krav til brukerautentisering, aksesskontroll, og integritet i systemene
Ref. ISO og EN standarder mht sikkerhet og spesifikt for vårt produktområde	Normalt så holder de seg til de internasjonale normer og standarder
Iht SIL- nivåer definert i EN50129	Iht SIL- nivåer definert i EN50128
Driftsstabilitet, krav til tilgjengelighet/oppetid	Ikke eksplisitt, men underforstått er det slike krav. SAT foretas alltid. Dette vil inkludere en test av eventuelle sikkerhetskrav.
Noen operatører stiller flere og strengere krav enn myndigheter	Lite krav i dag, krav forventes å øke
Lov, forskrifter, Europanormer	Lov, forskrifter, Europanormer
JA, Datasikkerhet (brannmur, inntregning etc.) i tillegg til pålitelighet/oppetidskrav	JA, Datasikkerhet (brannmur, inntregning etc.) i tillegg til oppetidskrav
Samme krav som myndighetene	Krav som myndighetene stiller
ja-mange	ja-mange
Ja, generelle krav til funksjon og konstruksjon gjort med tanke på å unngå ulykker.	Noen kunder har spesielle krav

Tabell 28: Bruker/kjøper/samarbeidspartneres krav til sikkerhet

Har bedriften kvalitetsikrings-rutiner som fokuserer på programvarepålitelighet/ sikkerhet?	**I hvilken grad er utvikling av sikkerhetskritiske systemer underlagt bedriftens sikkerhetsstyring?**
ja	Høyt prioritert ved f.eks. å involvere eksterne institutter til å validere og verifisere våre konstruerte sikkerhetsløsninger
ja	I liten grad
ja	Alle sikkerhetskritiske leveranser verifiseres internt av gruppen. Noen ganger brukes en uavhengig 3. part som TUV, Sintef, DNV
delvis	Sikkerhetsvurderinger foretas fortløpende i prosessen i h t bestemmelser om produktutvikling
ja	Underlagt QA system på navigasjon, ikke i samme grad på bakkeradar, kommunikasjon
Under innføring	Egen sikkerhetsstyring ble formalisert 01.01.01. All utvikling etter dette er underlagt ”sikkerhetshåndboka”
ir	ir
nei	ir
Ja, i form av koderegler	Adgangsbegrensning
ja	Gjennom instruksverket. Også organisatorisk der det er en veldefinert vei til ledergruppa i større prosjekter
ja	HMS styring, ikke spesielt på sikkerhet av programmerbare systemer
Ja, vi har bl.a. spesielle regler for modifikasjoner på sikkerhetssystemer, og jeg kan gjerne også nevne HAZOP analysene som brukes ved større modifikasjoner hvor man bl.a. ser på konsekvenser av at systemer feiler	-
ja	I tilstrekkelig grad
Ingen offisiell standard (som ISO) Følger egne rutiner	Ingen spesiell sikkerhetsstyring

Tabell 29:Oversikt over status når det gjelder bedriftenes kvalitetssikringsrutiner fokusert på programvarepålitelighet/sikkerhet

Utarbeides det sikkerhets og pålitelighetskrav til sikkerhetskritiske system?	**Baseres slike krav på risikoanalyser og behov for risikostyring og risikoreduserende tiltak?**
Utarbeides krav, i noen tilfeller utarbeides det krav til pålitelighetstall	ja
ja	ja
ja	ja
ja	ja
ir	ir
Ja, i spesifikasjonsfasen av nye prosjekter,	ja
ja	ja
-	-
Krav til sikkerhetsanalyse på et tidlig stadium i prosjektet. MIL-882D setter krav om sannsynlighet vs. konsekvens	Resultatet av sikkerhetsanalysen skal inngå i designbeskrivelsen
Ja, ifbm anskaffelse av systemer er dette et tema	Ja, i noen grad
ja	Nei, vi lager generiske krav som gir ulike produkter. Kravene kommer fra risikoanalyser gjort av kundene.
Har krav om pålitelighet/tilgjengelighet	Fra kundenes side, ja
ja	ja
ja	I samarbeid med kunden

Tabell 30:Oversikt over status for bedriftenes rutiner når det gjelder utarbeidelse av sikkerhets- og pålitelighetskrav

Utarbeides det en samsvarsvurdering i henhold til gitte sikkerhetskrav?
I noen tilfeller. Berøringsfare f.eks.
Samsvar mot maskindirektiv, klassekrav+ samsvar med spesifikasjon
ja
ir
ja
ir
Systemer for nedstenging av B&G deteksjon verifiseres og sertifiseres av TüV ihht. IEC61508. Uenig i at dette kreves i følge produsentansvarsloven
Mot MIL-882D
ja
Vi har foreløpig ingen spesielle aktiviteter som går på å måle eksisterende anlegg mot krav i IEC61508. Men Statoil har i 2001 gjennomført en total gjennomgang av teknisk tilstand på sikkerhetssystemene på samtlige anlegg i drift
nei
ja
ja
-

Tabell 31: Oversikt over i hvilken grad det utarbeides samsvarsvurdering

Har dere en dedikert person som er sikkerhetsansvarlig?
ja
nei
Ja på en av systemtypene, noen ganger på andre produkter/prosjekter
ja
Hver enhet har en sikkerhetsleder. Når det gjelder sikkerhetssystemene har vi definert et systemansvar som er tillagt operasjonssjef, men hvor daglig arbeid er tillagt navngitt person.
Nei – grupper av automasjonsfolk
Nei, men har det pr. prosjekt
ja
nei
ja
I alle større prosjekter
Ja, finnes overordnet kvalitetsikrings-system, men ikke detaljert ned som antatt i 61508
ja
ir

Tabell 32: Oversikt over i hvilken grad bedriftene har dedikert sikkerhetsansvarlig

Gjennomfører dere risiko og pålitelighetsanalyser av systemene?
• Komponentene gjennomgår FMEA og MIL217E beregning. Kritiske deler beregnes særskilt • Det gjøres FMEA og kalkulasjoner av standard produktløsninger • Det gjøres FMEA og kalkulasjoner av standard leverte systemer Det gjøres mindre på programvare
ja
I stadig større grad
ja
FMECA etc
Dette er helst knyttet opp mot bruken av systemene. Alle mulige funksjoner som har risiko knyttet til seg , blir testet ut til siste ledd i el-anlegget før idriftsettelse.
na
Krav fra kunden
I stor grad
ja
FMEA, noe risikoanalyser
Avhengig av type prosess og risikobilde

Tabell 33: Risiko og pålitelighetsanalyser

Mener dere at deres programmer kan inngå i et sikkerhetskritisk system?	**Vil dere kunne få rettslig ansvar hvis programmet medfører en ulykke?**	**Hvilke prinsipper anvendes i relasjon til risiko/pålitelighet (ALARP, kvantifiserte mål, inkrementelle forbedringer,)?**
ja	ja	
ja	ja	na
ja	ja	Krav til feilrate
ja	sannsynligvis	Ihht. IEC-61508 og SIL-ni
ja	ja	na
ja	Absolutt. Produktansvarslov. Spesielt viktig ved leveranser til USA.-	na
De gjør det	Muligens foretaksstraff	Det som er mest passende med hensyn på funksjon/teknikk.
Hyllevarene som produseres er ikke sikkerhetskritiske. (Tidsserie-databaser) Spørsmålet har ennå ikke vært aktuelt, men det kan bli det ved nye leveranser	-	
ja	Det har vi ingen erfaring med, men det er tvilsomt.	na
ja	ja	Ingen spesielle

Tabell 34:Spørsmål rettet til produsenter

I hvilken grad fokuserer dere på de spesielle utfordringene som gjelder for sikkerhet i programmerbare systemer?	**Har brukerne fått opplæring i de farer og risiko knyttet til bruken av systemer?**
Relevante punkter i EN 61508, EN 50126, EN 50128, EN 50129	nei
Vi fokuserer i første rekke på funksjonalitet. I dette ligger bla sikkerhet mot inntrenging utenfra, samt oppetidskrav og ytelse. Vi har ikke kompetanse til å mene noe om programinterne valg leverandøren gjør.	Brukerne av driftskontrollsystemet har flere måneders opplæring på systemet før de slippes til på egen hånd. De som ansettes har enten mange års erfaring som el-montør, eller er utdannet ing./siv.ing. med elektrofaglig studieretning.
Ganske stor grad	ja
I stor grad	delvis

Tabell 35:Spørsmål til brukerne

Vil det være mulig å spore tilbake hvordan det programmerbare systemet fungerte før og under hendelsen?	**Vil det være relevant å logge systemtilstanden og funksjoner på tilsvarende måte som man gjør i et fly (blackbox)?**	**Hva er praksis (state of the art) for de produkter som bedriften er relatert til?**
Til en viss grad	ja	?
Systemene kan i dag logge status i endel av delsystemene	Funksjonen brukes i normal operasjon i dag på de systemene som er dekket	Funksjonen brukes i normal operasjon i dag på de systemene som er dekket
Noen systemer umulig, noen systemer etter mindre tilpassinger, mens noen få systemer kan spores tilbake as is	ja	Logging av definerte systemvariabler ved endring og hvert sekund
Ja, delvis på flygelederkommunikasjon, ja for satellittnavigasjon, i liten grad for bakkeradar da det er sjelden kunden anskaffer et recordersystem for dette.	Ja, av myndighetene kun påbudt for talekommunikasjon. Gjøres for satellittnavigasjon, innebygget i systemet vi leverer. Sjelden for bakkeradar	Uklart spørsmål. Se over. Systemer som har vært involvert i en ulykke blir umiddelbart plombert av politiet.
nei	nei	ir
ja	ja	logging til historiestasjoner
ir	ir	ir
Det er vanskelig å gjennomføre	ja	Det gjennomføres datalogging av våpensystemer ved bruk i fredstid (militærøvelser etc.)
Ja det logges i en protokoll som ikke kan slettes	: Ja, for spesielt sikkerhetskritiske barrierer	Event logging med en protokoll som ikke kan slettes
ir	ir	ir
Stort sett mulig å logge de fleste parametre	ja	Kan gjøre logging, men varierende praksis
Gjennom hendelseslogger i systemet skulle det være mulig å komme et stykke på vei.	Det gjøres til dels (Operatørs inngrep logges i sanntid, samt status i systemet er logget i sanntid)	Dette skal være mulig i de fleste store og moderne driftskontrollsystemer som energibransjen benytter i dag. (Leverandører: Bl.a. ABB, Siemens og Telegyr)
Vanligvis	Vi bruker en alarmskriver, det kan kanskje sammenlignes med en ”black box”.	-

ja	ja	Felt analyse med kompetent personell, samt analyse av utskiftede komp.

Tabell 36: Oversikt over sporbarhet i etterkant av en ulykke

Har noen av personene som er involvert i utviklingen spesiell kompetanse når det gjelder utvikling av kritisk programvare?	**Henter dere inn sikkerhets-kompetanse fra eksterne leverandører/konsulenter?**
ir	nei
Noen få.	ja
-	Ja, bl.a. Sintef
ja	ja
ja	I noen grad
nei	nei
Det er generell kompetanse om programutvikling. Når det gjelder spesielle sikkerhetsaspekter er det folk innen bedriften med spesiell kompetanse som vegleder i utviklingsprosessen	ja
Lang erfaring med relesystemer, programvaren er kopi av relefunksjonalitet.	ja
nei	ja
ja	ja
ir	Ja, vi har ved et par anledninger hentet inn ekstern konsulent for å se på sikkerheten i vårt totale IKT-system – sist høsten 2000
ja	ja
ja	Behovsavhengig
Ikke spesiell formell kompetanse, men folk har lang erfaring	ja

Tabell 37:Personer med spesiell sikkerhetskompetanse

Hvilke kompetanse har dere når det gjelder utvikling av kritiske programmerbare systemer?	**Har dere behov for å øke kompetansen på disse områdene eller andre områder relatert til sikkerhet?**
Har en del kompetanse innenfor alle tema	Kunnskap om nye standarder IEC 61508
Utviklingsmetodikk Risikoanalyser Verifikasjon/validering/samsvarsvurdering.	ja
Utviklingsmetodikk? Bruker en metode basert på ”Unified software development process” (minner om RUP) Verifikasjon? generell verifikasjon	Ikke for øyeblikket, men det kan være relevant ved eventuell nye leveranser, f.eks. til legemiddelprodusenter
Risikoanalyser Verifikasjon/validering/ samsvarsvurdering	ja
ir	Ja, både vedlikeholde og utvikle
Har tilegnet seg noe kompetanse gjennom ett prosjekt når det gjelder alle temaene	Ja, dette skal være et satsningsområde
Det er generell kompetanse om programutvikling. Når det gjelder spesielle sikkerhetsaspekter er det folk innen bedriften med spesiell kompetanse som vegleder i utviklingsprosessen	Dette er viktig, men det er vanskelig å få folk med kompetanse. Sikkerhet er viktig for våre produkter
Noen kurs i sikkerhetsingeniør-utdanning ved NTNU	ja
ir	ja
Bedriften leverer, sammen med tysk partner, programmerbare systemer til både offshore og landbasert industri. Våre systemleveranser sertifiseres, som en hovedregel, til SIL2 og SIL3, avhengig av applikasjon. Pga. kapasitet gjennomføres en del av systemene mht. design, engineering, konfigurasjon osv. av oss her i Norge, mens andre utføres av samarbeidspartner. Vi er uansett ansvarlig for system design. Bedriften deltar ofte i risikoanalyser, men som regel ligger ansvaret for disse hos sluttbruker, og oftest med en uavhengig konsulent som ansvarlig for gjennomføringen. Dette på grunn av at en ren risikoanalyse av kun styresystemet, hvor kritisk det enn måtte være, blir meningsløst uten å se på prosessene rundt. Bedriften gjør ofte verifikasjon selv, særlig på mindre systemer, mens validering oftest utføres av en tredje part. Vi samarbeider tett med spesialist firmaer, særlig på større anlegg, for å gjennomføre nødvendige analyser av pålitelighet og tilgjengelighet. Vi har også utviklet et tett samarbeid med TUV Nord i Tyskland for uavhengig sertifisering av SIL3 anlegg. Samsvarsvurderinger er noe vi må gjennomføre for å	Ja, og dette vil fortsette å være høyt prioritert

kunne utstede samsvarserklæringer på leverte anlegg. Bedriften leverer også mange anlegg med trådbundet logikk, for de høyeste sikkerhets integritets nivåene. Dette er ikke programmerbare systemer, men inneholder mye av den samme metodikken med hensyn til gjennomføringen av et prosjekt	
Utviklingsmetodikk (noe på overordnet nivå) Verifikasjon/validering/ samsvarsvurdering	Størst behov for å overføre kompetanse fra satellittnavigasjonsavdeling til de andre produktområdene
Utviklingsmetodikk (noe på overordnet nivå) Verifikasjon/validering/ samsvarsvurdering	Ja,
Utviklingsmetodikk Risikoanalyser Verifikasjon/validering/ samsvarsvurdering	ja
Utviklingsmetodikk (noe på overordnet nivå) Risikoanalyser Verifikasjon/validering/ samsvarsvurdering	ja

Tabell 38:Oppsummering av svar om tilgang og behov for kompetanse relatert til utvikling av kritiske programmerbare systemer

I hvilken utviklingsfase trenger man mest å styrke kompetansen?
kravspek, testing,:
Kravspesifikasjon, operasjon
Spesielt på kravspesifikasjon og modifikasjon
Primært innen kravspesifikasjon og design
kravspek design utvikling
Kravspek, testing, validering og verifikasjon
design, testing
Modifikasjon
alle
Generelt om 61508
alle
Modifikasjon av applikasjon, testing
Kravspesifikasjonsfasen
Design og testing

Tabell 39: Svar på for hvilke utviklingsfaser man har størst behov for å styrke kompetansen

Innen bedriften	**I Norge generelt**
Kursvirksomhet Innleie av konsulenter	Utdanningstilbud Forskningsaktiviteter Internasjonalt samarbeid
Kursvirksomhet Spesialutdanning av sikkerhetsansvarlige ved intern kursvirksomhet. Nyansettelser Innleie av konsulenter	Spesielt viktig er det å få en utdanning som er nær knyttet til industriens behov. For eksempel ved trainee programmer, hovedfag eller doktorgrader direkte tilknyttet industriprosjekter
Kursvirksomhet Spesialutdanning av sikkerhetsansvarlige	Utdanningstilbud
Kursvirksomhet	Spesialfag eller fordypningsfag som diplom/hovedfagsarbeid. Interessert i internasjonalt samarbeid om standard internasjonale krav (viktig i forhold til at ikke norsk industri skal ha strengere krav enn utenlandske selskap).
”On the job training”, Innleie av konsulenter	Bør være en spesialiseringsgren på diplom/hovedfagsnivå, ikke et generelt studium
Spesialutdanning av sikkerhetsansvarlige	Utdanningstilbud
Spesialutdanning av sikkerhetsansvarlige Nyansettelser	Forskningsaktiviteter Internasjonalt samarbeid
Kursvirksomhet, Spesialutdanning av sikkerhetsansvarlige	Det bør settes inn større resurser for å bygge opp kompetansepersonell med en bredere forståelse av prosessen som skal ivaretas av et programmerbart sikkerhetssystem. Utdannelsen i dag synes å være nisjepreget og for teoretisk. Det skulle prioriteres en større andel praksis under studiefasen.
Spesialutdanning av sikkerhetsansvarlige (Bred kursing og bevisstgjøring)	Utdanningstilbud Forskningsaktiviteter Internasjonalt samarbeid Tror det er behov for å holde fokus på dette området generelt
Kursvirksomhet Spesialutdanning av sikkerhetsansvarlige Nyansettelser	Utdanningstilbud Forskningsaktiviteter Internasjonalt samarbeid
Kursvirksomhet Spesialutdanning av sikkerhetsansvarlige Nyansettelser	Utdanningstilbud Forskningsaktiviteter Internasjonalt samarbeid nasjonalt samarbeid
Selvopplæring	Utdanningstilbud
Spesialutdanning av sikkerhetsansvarlige Innleie av konsulenter	Utdanningstilbud Forskningsaktiviteter Internasjonalt samarbeid
Spesialutdanning av sikkerhetsansvarlige rundt våre virksomhetskritiske sanntidssystemer	-

Tabell 40: Bedriftenes svar på hvordan kompetansen bør utvikles

Hvilke problemstillinger synes dere at man bør fokusere på i et eventuelt framtidig forskningsprosjekt?	**Kunne dere tenke dere å delta i et slikt prosjekt?**
	Både indre kjerne og ytre referansegruppe
	Er i prinsippet interessert i å delta i en indre kjerne, men har vanskeligheter med å avse folk til dette
	Ja, med ca 1 månedsverk
	Ja, i en indre kjerne, delta med egeninnsats
	Interessert i å delta aktivt med støtte fra NFR på å overføre kompetanse fra satellittnavigasjonsmiljøet til de andre utviklingsmiljøene. Disse produkter har lavere krav til pålitelighet enn navigasjon. Forslagsvis med støtte på 150 knok per år.
Sikkerhetsmekanismer og sporbarhet	Ytre referansegruppe
Metodikk for verifikasjon/ validering av system leveranser innenfor jernbanevirksomhet	Indre kjerne
Primært på kravspesifikasjon, må lage enklere systemer som er lettere å operere og vedlikeholde	Ja, i en indre kjerne . Innsatsen vil avhenge av en definert utviklingsagenda
Dokumentasjon for drift og vedlikehold. Spesifikasjon av sikkerhetssystemer	Når det gjelder forskning så blir dette samordnet internt i bedriften. Området er meldt inn mot teknologiutviklings-programmet
Bruk av universelle produkter i stedet for spesialutviklede	Primært ytre referansegruppe, men kan også være aktuelt med indre kjerne
Gjenbruk, tillempe egnet utviklingsmetodikk, skalerbar prosess (etter sikkerhetskrav), estimering av utviklingsarbeid, bli flinkere til å fokusere på de viktige ting	Indre kjerne kan være interessert, men med begrenset omfang. Primært interessert i ytre referansegruppe
	Deltar allerede i flere NFR-prosjekter.
Modifikasjon og vedlikehold	Indre kjerne
	Ytre referansegruppe

Tabell 41: Behov for FoU i Norge innen sikre og pålitelige programmerbare systemer